Regulation Impact Statement (RIS)

Name of Department/Agency:	*Department of Home Affairs*
OBPR Reference Number:	25902

BACKGROUND

An interim Regulation Impact Statement was completed in May 2020. This Regulation Impact Statement builds on the interim Regulation Impact Statement to assess the high level regulatory impact to industry of uplifting the security and resilience of Australia's critical infrastructure. It includes further analysis of the proposed reforms, taking into account existing security measures, and includes a more in-depth analysis of the costs and benefits to industry, the community and the Government. If agreed, the Regulation Impact Statement will also support the introduction of legislation into Parliament. The legislation will outline what is required from industry and include sector specific thresholds to provide greater certainty to industry on which entities will be captured. The development of the reforms has been informed through industry engagement as detailed in section 5.

Sector specific rules are expected to be developed in early 2021 through a co-design process with industry. These rules will inform a more detailed regulation impact statement which will provide clarity around the costs and benefits of the specific obligations of the Risk Management Program for each sector and will form a key aspect of engagement with industry during this co-design process.

1. WHAT IS THE POLICY PROBLEM YOU ARE TRYING TO SOLVE?

1.1. Overview of the problem

The security of critical infrastructure is vital to Australia's social and economic stability, defence and national security. It enables the provision of essential services such as food, water, health services, education, energy, communications, transportation and banking. Without these services, our economic prosperity and public safety are threatened. The resilience of Australia's critical infrastructure is integral to the prosperity of the nation.

The existing framework governing critical infrastructure is being outpaced by an evolving threat environment as natural hazards become more prevalent, information technology and operational systems converge, the complexity of cyber threats grow, and foreign intelligence activities against Australian interests increase in frequency and sophistication. At the same time there are limited mechanisms in place to drive an uplift in all hazards risk management across all *critical infrastructure sector*s.

Without proper safeguards, security vulnerabilities in interconnected infrastructure can deliberately or inadvertently cause disruption that cascade across Australia's social and economic stability, defence and national security. While businesses have a strong incentive to ensure the resilience of their own critical infrastructure, the increasingly interconnected nature of critical sectors means that weaknesses within unprotected infrastructure can easily cascade and disrupt assets and systems vital to Australia's prosperity. As such, a wholesale uplift in security resilience is key to ensuring that *critical infrastructure asset*s are able to withstand significant compromise from a range of hazards.

The Department of Home Affairs (the Department) has undertaken industry focussed consultation to guide these reforms. Consultation considered the details of an enhanced critical infrastructure security regulatory regime, and how it should be approached. During consultation industry reaffirmed the lack of consistent national guidance available to assist in uplifting their security. As such, a wholesale uplift in all hazards security and resilience practices is integral to securing Australia's critical infrastructure. This will allow Australians to be assured that the Government is taking steps to manage threats to critical infrastructure and protect Australia's future.

1.2. What is critical infrastructure?

The 2015 Critical Infrastructure Resilience Strategy 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'.

Building on this definition, the Government intends to provide greater clarity on what is *regulated* as critical infrastructure. For the proposed reforms, *critical infrastructure sector*s are to be defined as:

***Critical infrastructure sector*s**	**Definitions**	**Examples**
Financial Services and markets	The sector of the Australian economy that involves: (a) carrying on banking business; or (b) operating a superannuation fund; or (c) carrying on insurance business; or (d) carrying on life insurance business; or	Banks, superannuation entities, financial market infrastructure.

	(e) carrying on health insurance business; or (f) operating a financial market; or (g) operating a clearing and settlement facility; (h) operating a derivative trade repository; or (i) administering a financial benchmark; or (j) operating a payment system; or (k) carrying on financial services business; or (l) carrying on credit facility business.	
Communications	The sector of the Australian economy that involves:: (a) supplying a carriage service; or (b) providing a broadcasting service; or (c) owning or operating assets that are used in connection with the supply of a carriage service; or (d) owning or operating assets that are used in connection with the transmission of a broadcasting service; or (e) administering an Australian domain name system.	Broadcasters, telecommunication companies.
Data storage and processing	The sector of the Australian economy that involves providing data storage or processing services on a commercial basis.	Cloud service providers, data centres.
Defence industry	The sector of the Australian economy that involves the provision of critical defence capabilities.	
Higher Education and research	The sector of the Australian economy that involves: (a) being a higher education provider; or (b) undertaking a program of research that: a. is supported financially (in whole or in part) by the Commonwealth; or b. is relevant to a *critical infrastructure sector* (other than the higher education and research sector)	Universities.
Energy	The sector of the Australian economy that involves: (a) the production, distribution or supply of electricity; or (b) the production, processing, distribution or supply of gas; or (c) the production, processing, distribution or supply of liquid fuel.	Liquid fuel includes crude oil and condensate, refined products such as petrol, diesel and jet fuels, and ethanol and biodiesel. Gas means 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.
Food and grocery	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.	Supermarkets, distribution centres.
Health care and medical	The sector of the Australian economy that involves: (a) the provision of health care; or (b) the production, distribution or supply of medical supplies.	Hospitals.

Space technology	The sector of the Australian economy that involves the commercial provision of space-related services. Note: The following are examples of space-related services: (a) position, navigation and timing services in relation to space objects; (b) space situational awareness services; (c) space weather monitoring and forecasting; (d) communications, tracking, telemetry and control in relation to space objects; (e) remote sensing earth observations from space; (f) facilitating access to space.	Ground stations, control centres.
Transport	The sector of the Australian economy that involves: (a) owning or operating assets that are used in connection with the transport of goods or passengers on a commercial basis; or (b) the transport of goods or passengers on a commercial basis.	Public transport companies, freight logistic companies, aviation and maritime entities.
Water and sewerage	The sector of the Australian economy that involves operating water or sewerage systems or networks.	Water utilities, desalination plants.

These definitions were designed through close consultation within industry, as outlined in detail in section 5.

1.3. Why is critical infrastructure important?

The above sectors are critical to the functioning and prosperity of Australia's social and economic stability, defence and national security. If any of these sectors or key assets within these sectors, are destroyed, degraded or rendered unavailable for an extended period, it would significantly impact the social and economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security.

Due to the increasingly connected nature of critical infrastructure, the impacts of compromises to critical infrastructure can spread rapidly across the economy with immediate and cascading consequences. For example, the consequences of a prolonged and widespread failure in the energy sector (through threats such as a cyber incident, weather events, or unlawful interference) could be catastrophic, causing:

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

1.4. What are the risks to critical infrastructure?

The primary objective of the reforms is to increase the resilience of Australia's critical infrastructure from all hazards. All hazard threats include both natural threats (including meteorological or weather events) and man-made threats (including unlawful interference, cyber incident, espionage, chemical or oil spills, trusted insiders) that have the potential to significantly disrupt critical infrastructure. Australia's social and economic stability, defence and national security are underpinned by secure and resilient critical infrastructure. Government, industry and the Australian public will have greater confidence in the resilience of Australia's critical infrastructure providers through a clear uplift in all-hazards risk management and contingency planning.

All hazard threats can be realised through inadequate protections within four key risk domains:

- **Physical** – the organisation's systems and networks, specifically protecting and mitigating them from natural, and human induced threats.
- **Cyber** – the digital systems, computers, datasets, and networks that underpin critical infrastructure system, and protecting them from cyber threats.
- **Supply chain** – the systems of organisations, people, activities, information, and resources that support Australia's critical infrastructure, and protecting their operations by understanding supply chain risk.
- **Personnel** – the employees, owners, operators, contractors, and subcontractors engaged with Australia's critical infrastructure, and the policies supporting these personnel.

The vital functions of critical infrastructure, such as the provision of electricity, food and health services, means that security must be considered from an all hazards approach, to ensure Australia's essential services and the Australian way of life is not disrupted or degraded, regardless of the source of a threat.

1.5. Increasing threats, connectivity and complexity of critical infrastructure

Critical infrastructure owners and operators, whether publicly or privately owned, operate in a market environment characterised by interconnectivity and an increasing reliance on technology. This connectivity and technology delivers efficiencies and economic benefits, but can also present new vulnerabilities when combined with the evolving critical infrastructure all hazards threat environment.

Vulnerabilities and increasing threats mean that a range of hazards have the potential to significantly compromise the supply of essential services across Australia. This year alone COVID-19 has demonstrated how quickly the consequences of significant incidents spread throughout the nation, with substantial security, social and economic impacts. During the COVID-19 pandemic there have been delays in a range of goods and services due to disruptions within different segments of supply chains, such as food and grocery delays due to interruptions at distribution centres.

An asset is only as strong as its weakest link. The interconnected nature of critical infrastructure means that a disruption to a *critical infrastructure asset* or their supply chains can have extensive, and costly externalities cascading beyond their immediate environment and network. It is not enough for an asset to have secure practices in place that protect them from all hazard threats, their supply chain must also be secure.

For example, disruption to the operability of the energy sector would have a significant domestic impact on the banking and finance sector.[1] This is due to the reliance the banking and finance sector has on the energy sector, through powering communications, online banking, automated teller machines, etc. Similarly, a significant disruption to the operability of the transport sector would have a cascading impact on the food and grocery sector. This is due to the reliance the food and grocery sector has on the trucking industry as the primary source of delivery for food and groceries to major distribution centres and supermarkets.

Prolonged disruptions to Australia's critical infrastructure can have severe flow on consequences to our economy, as demonstrated by several incidents of critical infrastructure disruption.

- A state-wide blackout in 2016, triggered by severe weather that damaged transmission and distribution assets, resulted in the suspension of the wholesale market in South Australia for

[1] Operability is defined as the ability of industry to keep its systems, networks, and infrastructure, functional to deliver goods and services at ordinary levels of productivity. An operability disruption is a disruption to the sector which results in the sector producing goods and services at a level below the ordinary level of productivity.

13 hours, costing an estimated $120,000 per minute for businesses operating in South Australia.[2]

- A Telstra outage in July 2019 impacted ATMs and EFTPOS machines across the country. According to National Retailers Association the five hour outage cost $100m in lost sales.[3]
- In 2018, a single morning peak hour disruption on the Sydney Harbour Bridge, caused by a member of the public climbing onto the bridge, resulted in disruptions that were estimated to have had an economic cost up to $10 million.[4]
- Costs of natural disasters in 2015 were estimated to be $9 billion, with an expected increase to $33 billion by the year 2050.[5]

The number all hazards impacting the operation of critical infrastructure through weaknesses in supply chains, personnel security, cyber connectivity, and physical characteristics are expected to increase over the coming years, especially within the cyber domain and from foreign intelligence services. The Australian Cyber Security Centre has reported that malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, sophistication and severity. Australia's Cyber Security Strategy 2020 noted that critical infrastructure providers were the victims of around 35 per cent of reported cyber incidents perpetrated by malicious actors in the year to 30 June 2020.[6] It is estimated that a four week interruption to digital infrastructures resulting from a significant cyber incident would cost the economy $30 billion (1.5 per cent of Australia's Gross Domestic Product) and around 163,000 jobs.[7]

Similarly, the Australian Security Intelligence Organisation's (ASIO) 2018-19 Annual Report identified that Australia continues to be a target for espionage and foreign interference. The report states that "Foreign intelligence services seek to exploit Australia's businesses for intelligence purposes" and "[t]hat threat will persist across critical infrastructure, industries that hold large amounts of personal data, and emerging sectors with unique intellectual property that could provide an economic or strategic edge".

1.6. Existing legislative arrangements are insufficient for the current threat environment

There are a range of legislative frameworks in place across *critical infrastructure sector*s that go to uplifting sections of critical infrastructure against aspects of all hazard threats. Many operators of critical infrastructure, particularly in the banking, finance, aviation, maritime and communications sectors already operate under regulatory frameworks that impose risk management, reporting and transparency obligations. Regulators in those sectors are already equipped to supervise those entities, identify emerging threats, and assist regulated entities respond to those threats. Existing regulatory frameworks often do not consider all hazard threats, and government powers are very limited in purpose and functions which do not meet security and resilience policy objectives. Some of the current regulators, frameworks and legislation includes:

- The Australian Energy Regulator regulates the Australian electricity and gas market. Their governance, functions, powers and duties include inspection and audit powers, however these powers are tied to the purposes and function of the *National Electricity Laws* and *National*

[2] AAP (2016) "SA blackout cost business $367 million", *SBS News*, https://www.sbs.com.au/news/sa-blackout-cost-business-367-million, viewed 24/08/2020
[3] Infrastructure Australia (2019) "Asset Management for Critical Infrastructure", <https://www.infrastructureaustralia.gov.au/listing/speech/asset-management-critical-infrastructure>, accessed 22/07/2020
[4] Wade, Matt & Clun, Rachel (2018) "Traffic chaos from Sydney Harbour Bridge drama cost city up to $10 million" *The Sydney Morning Herald*, <https://www.smh.com.au/national/nsw/traffic-chaos-from-sydney-harbour-bridge-drama-cost-city-up-to-10-million-20180404-p4z7rb.html>, accessed 22/07/2020
[5] Deloitte (2017) "Building resilience to natural disasters in our states and territories", <https://www2.deloitte.com/au/en/pages/economics/articles/building-australias-natural-disaster-resilience.html >, accessed 9/09/2020
[6] Australian Government (2020), "Australia's Cyber Security Strategy 2020", p.13.
[7] AustCyber (2020), "Australia's Digital Trust Report 2020", https://www.austcyber.com/resource/digitaltrustreport2020

Gas Laws. The Laws establish the key obligations surrounding the national electricity market, the regulation of access to electricity networks, access to gas pipelines and establishment of the gas market bulletin board to ensure reliable energy supply but critically, do not impose baseline all hazards risk reduction requirements on entities.

- The Aviation and Maritime Security (AMS) Division within the Department regulates the aviation and maritime transport sectors under the *Aviation Transport Security Act 2004* (ATSA) and the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA). These Acts (and their associated regulations) put in place a number of regulatory requirements on aviation and maritime operators to protect their operations from the threat of unlawful interference. In addition, security regulated airports, aircraft operators, regulated cargo agents, regulated ports, regulated ships, and regulated offshore facility operators are required to conduct security risk assessments. Security risks and vulnerabilities identified through these assessments inform the mitigation measures contained in a security plan that is submitted to AMS for approval. AMS also conducts compliance activities and has the power to impose infringements and penalties on operators who fail to comply with requirements. The ATSA and MTOFSA frameworks are not presently capable of applying in the context of naturally occurring risks to safety, human made risks to business operations, or risks which are otherwise not connected with unlawful interferences. The focus of existing legislative schemes is on security or safety of operations, not business continuity in a serious emergency. This means that the existing legislative schemes would not generally envisage the impacts of all hazards to the availability, confidentiality and integrity of aviation or maritime operations to be addressed.

- In New South Wales, the Independent Pricing and Regulatory Tribunal (IPART) is responsible for licencing arrangements some of which include critical infrastructure licence conditions such as physical and data security.[8] These licencing conditions were established in consultation with the Critical Infrastructure Centre (CIC) and do not exist in other states. These conditions also only apply for certain assets within the electricity and water sector, and not more broadly across all critical infrastructure.

- The *Security of Critical Infrastructure Act 2018* (SoCI) currently does not impose security obligations on *critical infrastructure asset*s (electricity, gas, water and maritime ports). Requirements on industry, such as reporting obligations, are limited and do not require them to take active steps to manage their security. While reporting is a useful mechanism to increase visibility of assets and notify the Government of potentially problematic changes, it does not improve all hazards risk management. The existing Ministerial directions power requires remediation action to improve asset security but these are reactive powers and are only applicable in the most extreme circumstances.

- The *Telecommunication and Other Legislation Act 2017* was passed to enhance security obligations for Australian carriers and carriage service providers (through the Telecommunications Sector Security Reforms). The Telecommunications Sector Security Reforms framework establishes a security obligation and notification obligation on industry, and provides the Government with an information gathering power and directions power. However, the Directions Power under s315A and s315B is not adequate to address time-sensitive security concerns. In order to exercise the Directions Power, the Australian Security Intelligence Organisation must provide an Adverse Security Assessment (ASA) in relation to the entity being directed, and the Direction must be given by the Minister for Home Affairs. Both of these processes can be quite lengthy and as a result could risk the direction not being able to be issued until well after the prejudicial security action has been taken by the offending entity. The current security obligations under the *Telecommunications Act 1997*

[8] Examples of licence conditions: https://www.ipart.nsw.gov.au/Home/Industries/Energy/Energy-Networks-Safety-Reliability-eand-Compliance/Electricity-networks/Licence-conditions-and-regulatory-instruments

also require Carriers and Carriage Service Providers to "do their best" to protect networks and facilities, but does not explicitly outline the specific security conditions which will be a core feature of the proposed reforms.

In other *critical infrastructure sector*s there is minimal regulation addressing all-hazards risks. For example, within the food and grocery sector, existing regulators are mostly focused on enforcing compliance with food standards, not in addressing threats from all hazards. Within the health sector, most entities are regulated at a state and territory level with minimal, consistent, overarching guidance from Federal Government, particularly against all hazards threats.

Where critical infrastructure owners and operators have taken positive voluntary steps to address all-hazards risks (such as improving cyber security arrangements), these can be ad-hoc and inconsistent across sectors. For example the Australian Cyber Security Centre's Essential Eight advises on broad baseline cyber security strategies that businesses can implement. However, entities are able to select the strategies they implement, how they implement them, and even whether they implement them at all, ultimately resulting in inconsistent standards across industry.

Without a clear and consistent approach it can be difficult for businesses to justify expenditure on uplifting all hazards security practices. This will increasingly lead to greater vulnerabilities being exposed in the nation's critical infrastructure. To ensure sector-wide resilience and security, industry must continue to adapt and keep up with the latest innovation and research. Without a more proactive stance on all hazards risk management there is a greater likelihood of critical infrastructure incidents. While certain *critical infrastructure asset*s may have mature security practices, they may rely on an industry or asset with less secure practices creating inherent vulnerabilities within their supply chains. This means that without a complete, sector-wide uplift in security the true benefits of reform cannot be realised.

If a significant cyber incident on critical infrastructure happened today, there is a risk that the Government may not have the mechanisms to act decisively to support an entity to stop or prevent an attack, nor does industry have obligations to report significant cyber incidents or apply minimum cyber security standards.

Foreign Acquisitions and Takeovers Act 1975

The inability of the Government to impose requirements on entities to protect their assets is a significant shortcoming in the current threat environment. This has created an over-reliance on the *Foreign Acquisitions and Takeovers Act 1975* (FATA) to manage risks. As the geopolitical environment continues to evolve, and as our national economy and critical infrastructure become ever more complex and interconnected, it is essential that the foreign investment review framework as set out in the FATA and the risk management framework under the SoCI adapt to meet these challenges. The critical infrastructure reforms look to compliment the FATA by providing an ownership agnostic risk management framework.

The Department is one of several national security partners the Treasury consults in preparing advice for the decision-maker on foreign investment applications under the FATA. CIC undertakes risk assessments on a case by case basis where an acquisition is in one of Australia's *critical infrastructure sector*s. Where national security risks are identified, the CIC may recommend imposing mitigations, which include a spectrum of binding conditions on the acquisition or, in the most extreme cases, that no conditions would manage the risk posed by the transaction.

Since the creation of the CIC in January 2017, there has been an average 61 per cent annual increase in critical infrastructure-related foreign investment applications being referred to the CIC for review. In the first year of its existence, the CIC assessed 242 cases (2017/18). Since then, case numbers have increased significantly with 626 cases assessed by the CIC in 2019-20. On 29 March 2020, the Treasurer announced temporary changes to Australia's foreign investment review framework in

response to the COVID-19 pandemic, setting a $0 monetary screening threshold for all proposed foreign investment in Australian businesses and land. The change resulted in a significant spike in the volume of applications referred to the Department for scrutiny, which it would not normally see under the regular monetary thresholds.

The proposed reforms within this RIS intend to address the increasing threats to our *critical infrastructure sector*s by placing obligations on critical infrastructure owners and operators to protect their assets against all hazards. This is designed to over time relieve the pressure on the foreign investment process, by allowing sector-wide obligations to take the place of case-by-case national security conditions. Sector-wide obligations will also ensure that foreign-owned and Australian-owned businesses are held to the same security standards. These reforms will, however, have limited effectiveness in mitigating risks where a foreign-owned entity is deliberately and deceptively acting to undermine Australia's national security. The changes contemplated in the FATA reforms will complement the critical infrastructure security reforms by effectively managing national security risk arising from ownership.

The proposed critical infrastructure enhanced framework will further align with the FATA reforms through a linked understanding of 'national security business'. The FATA Reforms proposes a new national security test which requires the mandatory notification of any proposed direct interest in a sensitive 'national security business' (including starting such a business). The definition of a national security business will be prescribed in the accompanying Regulation and will, among other things, include *critical infrastructure asset*s as defined in the SoCI.

1.7. The Government currently has limited visibility and power to act

Globally, we have recently witnessed a number of cyber security incidents in relation to *critical infrastructure asset*s 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 Ukrainian power outages on 23 December 2015 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 1% 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 away and passed away en route.

In Australia, current legislative regimes do not provide the Government with the ability to develop adequate visibility of threats to Australia's most significant systems (near real-time situational awareness), or provide directions to critical infrastructure entities in response to significant cyber incidents, if entities are unwilling or unable to resolve the incident.

As the majority of *critical infrastructure asset*s are owned and/or operated by the private sector, Government may not be aware of threats or cyber security incidents impacting industry and the Government has limited power to assist if it is not requested by the affected entity. This can result in delays that substantially impact the Government's ability to successfully assist in resolving an incident, especially when dealing with time sensitive matters such as cyber incident.

1.8. Regulation is wanted and needed to drive a wholesale uplift in security and resilience

Consultation for the Cyber Security Strategy 2020 highlighted that industry seeks greater direction from the Government in the protection of critical infrastructure. For the Cyber Security Strategy 2020, the Government:

- met with more than 1,400 people from across the country in face-to-face consultations, including workshops, roundtables and bilateral meetings; and
- received 215 submissions in response to the Cyber Security Strategy 2020 Discussion Paper.

The Government heard that Australia's critical systems are facing a worsening threat environment and the nation needs to address vulnerabilities in supply chain security, control systems and operational technology. This is consistent with advice from the national intelligence community and other sources.[9] Timely and actionable information sharing was identified as a critical gap.

To ensure sector-wide resilience and security, industry must continue to adapt and keep up with the latest innovation and research. Without a more proactive stance on all hazards risk management there is a greater likelihood of critical infrastructure incidents as industry is left to develop their own.

The Government values its ongoing engagement with critical infrastructure entities. Mechanisms like the Trusted Information Sharing Network (TISN) are important forums for cross sector dialogue, facilitating ongoing discussion on critical infrastructure resilience, including national security. Extensive engagement with industry and states and territories has revealed broad support for the introduction of an enhanced framework to secure critical infrastructure. Consultation on proposed reforms were conducted through six virtual town halls (attended by 620 representatives from business and civil society), 22 virtual workshops (attended by 949 individuals) and 194 submissions in response to the Protecting Critical Infrastructure and Systems of national significance Consultation Paper. This was further complemented by an additional four town halls and numerous bilateral conversations across industry as well as state and territory Government. A number of submissions were also received in response to a publically released exposure draft Bill.

Consultations highlighted that the Australian public looks to both the Government and critical infrastructure providers to secure the delivery of essential services. Collaboration and preparation ahead of time is needed so that everyone knows what their role is and what they need to do in an

[9] For example, see the Australian Strategic Policy Institute's report, *Protecting national critical infrastructure in an era of IT and OT convergence* (2019).

emergency. To do this, the Government and critical infrastructure entities need the right processes, authorisations and powers in place to respond rapidly and decisively.

2. WHY IS GOVERNMENT ACTION NEEDED?

2.1. Overview

The safe and secure functioning of Australia's critical infrastructure is essential to Australia's social and economic stability, defence and national security. Recognising the challenges outlined above, the existing regulatory framework across government is insufficient to manage the growing risks to critical infrastructure. The Government must act now to ensure a consistent and nation-wide uplift to the security and resilience of *critical infrastructure asset*s.

2.2. How can the Government successfully intervene?

The Government will work closely with industry to ensure that any reforms are directed at the most critical entities regardless of their ownership arrangements. This will achieve the broadest and most effective uplift and will create an even playing field for owners and operators. This will also maintain Australia's existing open investment settings, and ensure that businesses who take security seriously are not at a commercial disadvantage.

Ultimately, the objective of each option within the Regulation Impact Statement is to ensure that Australia has resilient critical infrastructure for the benefit of all Australians. This could be achieved through addressing the shortfalls in our current critical infrastructure framework and strengthen the Government's ability to:

- safeguard Australia's critical infrastructure against increasingly complex all hazards risks through increased industry responsibility;
- manage these risks collaboratively with industry through strengthened engagement and a more structured relationship with the owners and operators of our most critical systems (including cyber security activities to proactively identify vulnerabilities);
- identify and mitigate cyber threats to Australia's most critical systems through increased situational awareness of the threat environment;
- provide directions to industry where necessary in response to cyber incidents;
- respond rapidly in exceptional circumstances by making it clear what the Government is authorised to do; and
- maintain Australia's open investment policy settings, when in the national interest, in an ever evolving geopolitical and economic landscape.

2.3. Externalities

The increasingly interconnected nature of critical infrastructure means that disruption to *critical infrastructure asset*s or their supply chains can have extensive and costly externalities. While an entity may have stringent security practices in place, if a third party responsible for a core component of their supply chain is not secure, it can have cascading and damaging effects. For example, while a hospital may have secure cyber practices, a data centre that holds their patient data may not. As such, a compromise within a data centre could have cascading effects on a hospital, even though a hospital itself has done everything in its power to secure its patient records. Consequently, market forces are not sufficient to safeguard all critical infrastructure against all hazard threats. Government action is needed to provide greater assurance that vulnerabilities are proactively detected, prevented and any realised incidents impacting Australia's critical infrastructure are resolved without negatively influencing Australia's social and economic stability, defence and national security, or the reliability and security of other *critical infrastructure asset*s.

3. QUESTION THREE: WHAT POLICY OPTIONS ARE YOU CONSIDERING?

The Department has considered three broad options to address the identified problems:

Option 1: Maintaining the existing arrangements without amendment.

Option 2: Strengthened government regulation, enhanced compliance and voluntary engagement through the TISN for Critical Infrastructure Resilience.

Option 3: No legislative change, achieve improvements to critical infrastructure resilience with voluntary engagement through the TISN and publishing additional guidance alongside the updated Critical Infrastructure Resilience Strategy

The detailed costs and benefits of all three options are provided within section 4.

3.1. Option One – No regulatory change or enhanced compliance

This option involves no legislative reform and maintaining the status quo of the TISN, the Australian Cyber Security Centre and their Joint Cyber Security Centres. The Government would have no direct involvement or influence over the security practices of owners and operators of *critical infrastructure asset*s in Australia, have little understanding of Australia's most vital systems beyond water, electricity, gas and maritime ports, and lack the ability to source real-time situational awareness or assist industry to prevent or respond to threats in exceptional circumstances. Owners and operators would continue to have minimal security requirements in many *critical infrastructure sector*s.

This approach would not address the current risk to critical infrastructure outlined within section 1.

3.2. Option Two – Strengthened government regulation, enhanced compliance and voluntary engagement through the Trusted Information Sharing Network for Critical Infrastructure Resilience

Option two involves legislative amendments to SoCI to enhance existing powers, combined with revitalising the TISN and releasing a new Critical Infrastructure Resilience Strategy. Collectively these measures will go to addressing the problems defined within section 1, helping to reduce the risk and consequence of security incidents.

Option two will introduce a range of regulatory obligations and non-regulatory mechanisms for three broad classes of entities:

1. *Critical infrastructure sectors* – as defined within section 1.2;
2. *Critical infrastructure assets* – a specific subset of assets within *critical infrastructure sector*s that will be defined within SoCI. The thresholds for *critical infrastructure assets* are further explained in Attachment A;
3. *Systems of national significance* – those assets declared by the Minister for Home Affairs to be most critical to Australia's social and economic stability, defence and national. These systems will be a specific and limited subset of *Critical infrastructure assets*. It is proposed that SoCI be amended to allow the Minister to declare, in writing, that a particular asset is 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 having considered:
        - the extent of shared interdependencies of the asset across the economy; and

- any other matters the Minister considers relevant.

The Minister for Home Affairs will be able to declare a *system of national significance* once legislation has passed. However, it is proposed that there will be a consultation requirement within the legislation dictating that the Minister for Home Affairs must first consult with an entity before declaring it a *system of national significance*.

The four elements of the enhanced framework under Option Two include Positive Security Obligations, Enhanced Cyber Security Obligations, Government Assistance and Ministerial Directions as further detailed below. The following entities will be subject to each of the measures:

	Entities within C*ritical Infrastructure Sectors*	***Critical Infrastructure Assets***	***Systems of National Significance***
Positive Security Obligations*	No	Yes	Yes
Enhanced Cyber Security Obligations	No	No	Yes
Government Assistance	Yes	Yes	Yes
Ministerial Direction	No	Yes	Yes

* The obligations under the Positive Security Obligations will need to be "turned on" (through the making of a rule) for each class of assets, meaning that there will be no regulatory burden experienced by industry under the Positive Security Obligations until defined within the Rules.

3.2.1. Positive Security Obligations is the collective name for three regulatory obligations intended to uplift the security and resilience of *critical infrastructure asset*s, build cyber situational awareness and enable the Government and industry to more effectively prevent, defend against and recover from all hazards. These obligations will apply to *critical infrastructure asset*s and each of the obligations will need to be explicitly turned on (through the making of a rule) for each asset or class of assets. This will be used to offset potential regulatory burden through managing any potential areas of duplication with existing arrangements, recognising equivalent regimes that are already in place. There will be three distinct obligations within the Positive Security Obligations:

- *Register of Critical infrastructure asset* – Part 2 of the current SOCI created a Register of *Critical infrastructure asset*s which was designed to assist the Government in gaining greater visibility of who owns, controls and has access to *critical infrastructure asset*s, including board structures, and outsourcing and offshoring information ultimately ensuring the security and resilience of critical infrastructure. The Register requires reporting entities, who are either direct interest holders or the responsible entity of *critical infrastructure asset*s, to provide interest and control information and operational information to the Secretary within a certain timeframe. The number of entities required to report to Register is expected to increase in conjunction with the expanded definition of *critical infrastructure assets.* However, the obligation to report to the register will not be activated until the Minister for Home Affairs, through the rules, has activated the obligation for particular *critical infrastructure asset*s after consultation with industry. This is intended to prevent duplication, offset the potential regulatory burden experienced by industry by not requiring further reporting on top of existing obligations.

The expansion of the Register will be in line with existing protections already in the SoCI Act, consistent with the Australian Privacy Principles

The Government recognises that a range of mechanisms to manage certain hazards already exist. The Government does not propose to duplicate or replace these existing mechanisms but instead will work with key stakeholders (including industry, peak bodies, regulators, and state and territory governments) to leverage existing regulations and frameworks, and where necessary build on them to deliver a more consistent approach to managing risk across all sectors. This will be achieved through deferring to existing regulatory obligations where they are equivalent to components of the risk management obligations.

- *Critical Infrastructure Risk Management Program* – under this obligation, assets that are considered *critical infrastructure asset*s will be required to develop and comply with a critical infrastructure risk management program. The program is intended to increase resilience across critical infrastructure assets, address vulnerabilities across physical, cyber, supply chain and personnel domains, provide a wholesale uplift in the security of critical infrastructure and reassure Government that critical infrastructure assets are appropriately safeguarded against all hazard risks (as explored in section 1).The Bill will set out the overarching obligations for the risk management programs with the more detailed, sector-specific requirements to be contained within the rules. The risk management program will require a responsible entity of a *critical infrastructure asset* to identify material risks to their asset, propose a plan to mitigate risks so as to prevent incidents, minimise the impact of any realised risks and have appropriate risk management oversight arrangements in place for their program. The Minister for Home Affairs, through the rules, will be required to activate the obligation for *critical infrastructure asset*s.

  The Minister for Home Affairs will also have a rule making power to specify how an entity must meet these security obligations. These rules will be legislative instruments and disallowable by Parliament. Sector-specific rules will be co-designed with industry to provide clarity around expectations, and what would be considered a reasonable and proportionate response to meeting the obligations. Following commencement and the enactment of sector-specific rules, industry would be provided a grace period during which they are legally obliged to comply with the obligation but no enforcement action can be taken. This will provide industry time for the necessary uplifts to occur with the support of extensive outreach and education from the CIC.

  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 90 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.

All costs associated with the critical infrastructure risk management program will be costed within future RIS(s) – including the costs associated with an entity's obligation to report annually to the Secretary of Home Affairs.

- *Notification of cyber security incidents* – the responsible entity of a critical infrastructure asset, who is not subject to an equivalent obligation elsewhere, will be required to report cyber security incidents which involves a direct compromise of the system or impacts the functioning of the asset.[10] This obligation imposes a two-tiered reporting obligation on the responsible entity for a *critical infrastructure asset* based on the severity of a cyber security incident. The first tier is where an entity is experiencing a cyber security incident that has had, or is having, a significant impact on the availability of the asset and must report the incident within 12 hours of the entity becoming aware of the incident.[11] The second tier is where an entity is experiencing a cyber security incident that has had, is having, or is likely to have, a relevant impact on an asset and must report the incident within 72 hours of the entity becoming aware of the incident.[12] The reports must be made to the Australian Cyber Security Centre (unless another Commonwealth body is prescribed in the rules), and made orally or in writing. For example, the entity will be required to report the detection of malware on their system or a denial of service attack that disrupts the service, but not phishing emails that do not have an impact on the entity. These reporting obligations are only engaged (i.e. the clock starts) when the entity becomes aware of the incident, and therefore may not be activated until sometime after the incident has occurred and an internal investigation has revealed the source of the problem.

  These reports will be used by the Australian Cyber Security Centre:
  - where appropriate, to initiate an offer of assistance or in particularly serious situations, an application for government assistance (discussed below), and
  - provide intelligence to support the development of an improved national situation awareness.

  This obligations will provide Government with greater visibility of the current cyber environment that critical infrastructure assets are operating within, allowing Government to develop an aggregate threat picture which can then be used to inform industry of, and assist industry to deal with, the threats they face.

  The Bill will define the obligations, however the Minister for Home Affairs, through the rules, is required to activate the obligation for particular *critical infrastructure asset*s.

3.2.2. Enhanced Cyber Security Obligations will only apply to assets which are considered to be of the highest criticality (*systems of national significance*). These obligations are intended to build upon the existing strong Government-industry partnership and provide the Government with the information and understanding necessary to reduce the risk and potential impacts of significant cyber incidents. It will also provide the Government with assurance that assets of the highest criticality are actively safeguarding their assets from cyber vulnerabilities above

[10] In order to cost the notification of cyber security incidents for industry a total maximum cost is calculated where all critical infrastructure entities required to report cyber breaches, acknowledging that this may not be the case where equivalent obligations already exist.

[11] What is considered a 'significant impact' is likely to vary between assets and across sectors and it will be up to the entity to determine when a *relevant impact* is significant for the purposes of this reporting obligation.

[12] 'Relevant impact' means a direct or indirect impact on the availability, integrity, reliability or confidentiality of a critical infrastructure asset, information about the asset, or data or information stored in the asset.

and beyond their requirements under the Positive Security Obligations. Due to the increasingly interconnected nature of critical infrastructure, it is vital that those of the highest criticality (*systems of national significance*) are actively safeguarding against significant cyber security incidents to reduce the occurrence and impacts of such incidents. The Minister for Home Affairs will provide an annual report to Parliament on the use of these powers. There will be four distinct components of the Enhanced Cyber Security Obligations which will be activated only on request (meaning there is no standing obligation):

- *Develop and maintain incident response plans* - under this obligation the Secretary may require the responsible entity for a *system of national significance* to establish and maintain an incident response plan. Incident response plans are designed to ensure an entity has established processes and tools to prepare for and respond to cyber security incidents. It is intended that the plan would need to 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. An incident response plan typically includes profiles of common incident types and response activities for the organisation and sector, roles, responsibilities and contact details, and checklist of actions (for detection and analysis, containment and eradication, communications and recovery) and templates to use when required. Engagement with industry has indicated that many *systems of national significance* are likely to already have an existing incident response plan that can be provided to the Government upon request.

- *Undertake a scenario based exercise* - under this obligation the Secretary may require the responsible entity for a *system of national significance* to undertake a cyber security exercise. It is intended that the Secretary of Home Affairs may, by written notice, require a *system of national significance* 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). Conducting a cyber security exercise is an important activity for an organisation to test and improve their cyber resilience. The scope of the exercise will be determined based on 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. This is intended to test an entity's ability to respond appropriately to a cyber security incident, preparedness to respond to a cyber security incident and ability to mitigate relevant impacts of a cyber security incident.

- *Conduct a vulnerability assessment* - under this obligation the Secretary may require the responsible entity for a *system of national significance* to undertake a vulnerability assessment. 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. 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 and the requirements of the assessment will be outlined in the request made by the Secretary. This assessment can be undertaken by the entity or a third party on behalf of the responsible entity. Where an entity is unable to conduct an assessment, Government may also to undertake a vulnerability assessment of the asset on the assets behalf.

- *Provide access to system information relating to the functioning of a system* - An organisation's ability to detect and respond to a cyber incident depends on having visibility across their technology environment. This visibility is provided in the form of telemetry (often referred to as system logs or systems information) that are usually aggregated into a centralised security operations capability. Under the ECSO, the Secretary may require the responsible entity for a *system of national significance* to provide such system information. 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.

  If an entity is requested to provide access to telemetry (host, gateway, etc), they could utilise existing arrangements or procure relevant technology. Most large organisations are likely to have an already established cyber security function or existing engagement with a cyber security service provider. This information could be streamed or dumped. Software delivers this function and can be configured as required. The 'serviceability' of this software is likely within the ability of in house IT functions. After initial set up/deployment, monitoring the serviceability and maintenance of the software could easily be integrated into BAU practices. If in house cyber security wanted to use the program for their own monitoring (other than to undertake this obligation), then this would likely be integrated into BAU processes as well. The type of technology required will vary between networks.

  Importantly information able to be requested under these obligations will be limited to information about networks and systems and not information about consumers. Any incidental personal or commercially sensitive information collected will be subject to the Australian Privacy Principles and principles on data minimisation, to the greatest extent possible. Notifiable data breaches will be reported to the Office of the Australian Information Commissioner.

3.2.3. Government assistance to relevant entities within *critical infrastructure sectors* in response to significant cyber attacks that impact on Australia's *critical infrastructure assets*. Entities outside of *critical infrastructure sectors* will not be subject to these measures. Entities are primarily responsible for managing cyber security risks through calibrated risk management, preparatory activities and enhanced situational awareness. However, in exceptional circumstances, the enhanced framework will provide the Government with the power to take appropriate steps to prevent and address cyber security incidents that threaten serious prejudice to Australia's interests, mitigate the impacts of such incidents on critical infrastructure, and restore the functioning of those assets. These powers will provide Government with the power to act in exceptional circumstance in order to protect our nation's critical infrastructure assets. This will be achieved by enabling the Minister for Home Affairs to authorise the Secretary of Home Affairs to issue an *information gathering direction*, an *action direction* or an *intervention request* (as explained below).

Importantly, prior to authorising the Secretary of Home Affairs to issue directions to a critical infrastructure asset, the Minister for Home Affairs would need to be satisfied that:

- a cyber security incident has occurred, is occurring, or will imminently occur

- the incident has had, is having, or is likely to have, a relevant impact on a *critical infrastructure asset*
- there is a material risk that the incident has, is, or is likely to, seriously prejudice:
  - the social or economic stability of Australia or its people, or
  - the defence of Australia, or
  - national security, and
  - no other existing Commonwealth, State or Territory regulatory regime could more effectively be used to respond to the incident.

In considering an application in relation to the exercise of information gathering, action direction or intervention powers, as a matter of practice, the Minister for Home Affairs will notify other relevant Commonwealth Ministers at an appropriate time. Those other Ministers may choose to make representations to the Minister for Home Affairs or Prime Minister to support their respective decisions. An operational protocol, to be agreed by Government, will be developed to support the implementation of this regime and will expressly articulate procedures for consultation, including for example, circumstances where the Prime Minister would call a meeting of the National Security Committee of Cabinet or consultation with relevant regulators to coordinate action. This will allow the Government to determine the most appropriate way of ensuring relevant Ministers are involved in the decision making process.

Furthermore, an authorisation made for directions or intervention powers will cease after 20 days, unless the Minister for Home Affairs has revoked the authorisation earlier due to the resolution of the incident or compulsory powers no longer being required. Where an emergency continues beyond this time period, the Minister for Home Affairs may make another authorisation in relation to the particular incident if satisfied of all the necessary criteria. In the event that the Minister for Home Affairs seeks another authorisation to a particular event, the Minister for Home Affairs will again require the agreement of the Minister for Defence and the Prime Minister.

Under the Government Assistance measures the Minister for Home Affairs to authorise the Secretary of Home Affairs to do one or more of the following:

- *Information gathering direction* – the Secretary may require the responsible entity for an asset within a *critical infrastructure sector* to provide information in order to support the Minister for Home Affairs' decision as to whether to pursue further direction or intervention powers (as discussed below) in light of a cyber security incident. Importantly, 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 or is reasonably possible to execute. This direction would only be made upon suspicion of a cyber-crime having occurred, occurring, or occurring imminently.

  An entity is not excused from giving information in response to a direction if the information could potentially incriminate the entity and 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 to better understand the situation to facilitate a better response to an incident.

Scenario (information gathering direction):

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.

The Minister for Home Affairs would authorise the Secretary to issue an information gathering direction to the supplier, to provide the necessary information. This information could be used to jointly develop an appropriate response with the responsible and determine whether further Government assistance is required to mitigate the incident.

- *Action direction* – the Secretary may require the responsible entity for an asset within a *critical infrastructure sector* to prevent a cyber security incident, mitigate the impact of the incident, or restore the functionality of a *critical infrastructure asset* affected by the incident. The Secretary will also be required, if practicable, to consult with the responsible entity prior to making any direction to ensure a proper understanding of potential unintended consequences, and may consult with relevant Commonwealth agencies in determining necessary actions. In practice, the Secretary of Home Affairs will work closely with relevant agencies to determine necessary directions. For example, the Australian Signals Directorate may advise the Secretary that a relevant software patch is likely to be effective in preventing an imminent incident, advice which forms the basis of the Secretary's direction.

  The Minister may authorise the Secretary making directions which:

  - are prescribed in the legislation and are reasonably necessary and proportionate to achieving the objective of resolving the incident, or
  - such other directions as the Minister for Home Affairs expressly authorises and are reasonably necessary and proportionate to achieving the objective of resolving the incident.

  If a direction is required which is not prescribed, or has not been directly authorised, the Secretary would need to return to the Minister for authorisation to make such a direction. This allows the flexibility to respond to a fast-moving cyber emergency, while ensuring the Minister retains oversight of directions being made.

  The ability to direct the entity to provide a government official with direct access to a network will be expressly excluded to ensure it cannot be used as a backdoor to these powers.

  It is not proposed that directions can be issued to private sector entities who are not otherwise connected with the operation of the asset as it would not be appropriate to compel an unconnected third party. Rather any direction to a related critical infrastructure sector asset must be necessary to respond to the incident and if the entity cannot respond appropriately, direct intervention should be limited to the Government to minimise impacts on the privacy of the asset.

  It will be a criminal offence for an entity to fail to comply with a lawfully issued direction. Noting this, the entity, or officers acting on its behalf, will be provided with immunities from any civil claim when acting in accordance with such a direction. Similarly, an industry provider that provides voluntary assistance in line with a request will be provided immunities from any civil claim. This will support the Government receiving the necessarily technical advice in an emergency.

- *Intervention request* – in the event that an entity is not responding to an information gathering direction or an action direction, the Secretary would be able to request assistance from, the Australian Signals Directorate through the exercise of intervention request powers in relation to a cyber incident. Essentially, this will be a last resort power and would also require the agreement of the Minister for Defence and the Prime Minister. This intervention request will be limited to the ASD accessing an entities computer, undertaking analysis of computer data, altering data

held in a computer and altering the functioning of a computer. This serves as a limiter to ensure that the actions are computer-related acts and appropriately targeted as responding to the cyber security incident.

The use of force against a person or offensive cyber activities (for example, hacking back) will be expressly prohibited from occurring under the Government Assistance portion of this regime. The Australian Federal Police will support the Australian Signals Directorate in the exercise of these powers as required, including using force to gain entry to a premise.

Noting the complexity of a nationally significant cyber security incident and the systems being impacted, it is crucial that any direct action taken by the Government is done by experts to ensure quick resolution with limited collateral impacts. Officers of the Australian Signals Directorate will remain subject to any relevant legislation, as well as their own organisation and ministerial oversight arrangements when considering and responding to a request for cooperation or assistance.

It is a criminal offence, under section 149.1 of the Criminal Code, for a person to hinder or obstruct a Commonwealth officer in the exercise of their powers. A person obstructing an Australian Signals Directorate official exercising powers under this regime would be liable to imprisonment of up to 2 years.

Officers of the Australian Signals Directorate, including any industry contractors that are engaged by the entity through the Intelligence Services Act 2001, will be provided with immunity from any civil claims when exercising Government Assistance powers at the request of the Secretary. Further, those officers will also be provided criminal immunities when acting in good faith in compliance with lawful authority, similar to those provided under other domestic intelligence and law enforcement regimes. Noting the express exclusion of the use of force against a person, the criminal immunities will not extend to conduct that is intended to cause death or serious injury to any person.

It is proposed that are a range of safeguards be included to ensure that an intervention request only occurs as a last resort. These safeguards include the need for the Minister for Home Affairs to be satisfied that the entity is unwilling or unable to take all reasonably necessary steps to appropriately resolve the incident. The Minister for Home Affairs must not make such an authorisation unless satisfied that the request is reasonably necessary for the purpose of responding to the incident, the specified request is a proportionate response to the incident, and the authorisation of an action direction would not be practical or effective response to the incident.

Scenario (action direction and intervention request):

During an 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, 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 action direction relating to each of these specific actions. Where an action direction is not actioned by the respective entity (either through a refusal to do so, or a lack of capability), then an intervention request relating to each of these specific actions.

Oversight

The Commonwealth Ombudsman, within its current mandate, will have the ability to receive, consider and take action in relation to complaints made by an entity in relation to a direction issued by the Secretary of Home Affairs under this power or the Australian Federal Police's actions in supporting the Australian Signals Directorate. The Inspector-General of Intelligence and Security, within its current mandate, will have the ability to oversight any exercise of the Government Assistance powers by the Australian Signals Directorate as well as any advice provided to the Secretary of Home Affairs by an intelligence agency within its jurisdiction to support the making of a direction. Information sharing provisions will be included to ensure these two oversight bodies can work effectively together. The oversight powers of the Inspector-General of Intelligence and Security in relation to the regime will be significantly greater than those of the Ombudsman, which is proportionate to the nature of the respective powers over which they have supervision.

The Secretary of Home Affairs will be required to provide the Minister for Home Affairs a report on the exercise of powers under the authorisation including how they contributed to the resolution of the cyber security incident and an assessment of any prejudice caused. Where Government Assistance powers were used, this report will be copied to the Minister for Defence and the Prime Minister.

It is proposed that the ministerial authorisation, and administrative decisions made in accordance with that authorisation, will not be subject to judicial review under the Administrative Decisions (Judicial Review) Act 1977 or obligations to consult the relevant entity prior to making the authorisation. This is reflective of the emergency nature of these powers, national security information that will used to satisfy the various decision makers, and their connection with the protection of Australia's national security, defence, economy and social stability. However, the bias rule aspect of procedural fairness will be unaffected, and judicial review will remain available by way of section 75(v) of the Constitution and section 39B of the Judiciary Act 1903.

3.2.4. Ministerial Direction power

Option 2 would also include expanding the assets to which the current Ministerial Direction within the SoCI may apply.[13] Current section 32 of the SoCI allows the Minister for Home Affairs to issue a direction to an owner or operator of a *critical infrastructure asset*. The primary purpose of this existing directions power is to ensure that, as a last resort, the Government can address risks to *critical infrastructure asset*s that are prejudicial to security (within the meaning of the *ASIO Act 1979*).

For example, a Ministerial Direction may require a business to limit any offshore access to its industrial control systems unless approved by Government where underlying security risks,

[13] Increasing the number of entities subject to the power from approximately 167 critical infrastructure assets to 1,700 critical infrastructure assets.

such as the potential for extrajudicial influence, are identified. This scenario is costed with section 4 of the RIS.

The expansion of the Ministerial Directions power will ensure the Government has the necessary powers to address security risks across all critical infrastructure assets, including the newly defined *critical infrastructure assets* proposed under this reform, where these cannot be managed through other mechanisms. The current SOCI explicitly mandates that the Government must consider the use of existing mechanisms, including state and territory regimes, before issuing a direction. This mandate provides safeguards that will ensure the power is used appropriately and not exercised beyond the remit of specific risks that are prejudicial to security that cannot be addressed through other means. Further stringent safeguards include the need for the directions to only be issued in connection with the operation of a critical infrastructure asset or the delivery of a service by a critical infrastructure asset, where there is a risk of an act of omission, and that the risk would be prejudicial to security

The Government Assistance measures are a necessary in addition to the expansion of the Ministerial Direction powers in order to respond to fast moving and significant cyber security incidents affecting *critical infrastructure assets.* While Ministerial Directions can only be issued to *critical infrastructure asset*s and their operators, Government Assistance measures are intended to be directed at an asset within a *critical infrastructure sector* that is impacting a *critical infrastructure asset*s. This allows measures to be directed at the entity best placed to respond to an incident. This reflects the complex and interconnected nature of Australia's economy where the functionality and operability of *critical infrastructure assets* are dependent on the services of a variety of assets within *critical infrastructure sectors*. In particular, this relationship is often dependent on, or facilitated by, an interconnected digital network or internet-connected systems.

Voluntary engagement through the Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN)

The proposed measures are intended to leverage and enhance existing regulatory frameworks, and will be enriched by enhanced government-industry engagement and collaboration through the TISN.

The TISN was established in 2003 and is the primary voluntary engagement mechanism for industry-government information sharing and resilience building initiatives. The refreshed TISN will better support the wide-ranging regulatory reforms to SoCI*,* reflecting the increased interdependency of *critical infrastructure sector*s. The success of the regulatory changes outlined above will be underpinned by enhancements to the network, which include greater engagement, education, guidance and collaboration with industry.

The TISN will support the implementation and delivery of the proposed reforms to SoCI by providing a forum to co-design sector specific regulations and best practice guidance to ensure the obligations are fit for purpose and to support industry to comply with its obligations. The TISN will expand the number of sector groups to better support the range of critical infrastructure owners and operators in the 11 identified *critical infrastructure sector*s, reflecting the broader regulatory environment. The TISN structure will also provide greater opportunities for cross-sector collaboration, in recognition of increasing sector interdependencies. This approach will encourage all affected entities, large and small, to participate in the design process and ensure the resulting regulations provide a level playing field for all participants. It will also enable members to better understand, and therefore fulfil, their regulatory responsibilities, which will result in a decrease in the need and cost of compliance activity.

By facilitating government-industry engagement across a broader range of sectors and issues, owners and operators of *critical infrastructure asset*s will have an improved ability to ensure continuity of service of *critical infrastructure asset*s in the face of all-hazards.

The refreshed TISN will also help achieve the objective of the new *Critical Infrastructure Resilience Strategy* (due for release in early 2021) to establish a common understanding of critical infrastructure resilience and to promote critical infrastructure that can withstand and mitigate the effects of all hazards and to quickly return to service after any periods of disruption.

Compliance and enforcement

The Department, as the primary regulator, will have various monitoring and investigation powers to support compliance and enforcement activities. In addition to those powers already contained in SoCI, Parts 2 and 3 of the *Regulatory Powers (Standard Provisions) Act 2014* will be activated in relation to provisions of SoCI. These powers will also be able to be conferred on another relevant Commonwealth regulator where it is determined that they are best placed to regulate compliance with the obligations in a particular sector.

These monitoring and investigation powers will be supported by a series of civil penalties and criminal sanctions which attach to non-compliance with the obligations under the Act. Civil penalties range from 150 to 200 penalty units per day of non-compliance. This is to ensure that the penalties associated with the new obligations are proportionate to the existing penalties within the current SoCI as well as reflect the seriousness of inaction and dissuade entities from not meeting their obligations.

The amendments will provide the Department or alternative regulator, with a range of graduated enforcement options which can be scaled to address the particular circumstances of 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.

It is proposed that the Department will take a risk based approach to compliance and enforcement by prioritising monitoring of assets based on their criticality, with more proactive monitoring focused on *systems of national significance*.

The expansion of Government powers and regulations necessitate significant transparency and oversight. Consequently, it is proposed that the Department would expanded its reporting requirements to Parliament under the current SoCI to include all proposed new measures and powers. This would enable Parliamentary scrutiny as well as provide public oversight on the extent of actions being undertaken by the Government under the powers granted under the proposed reforms. Under current SoCI the Secretary must give the Minister, for presentation to the Parliament, a report on the operation of SoCI for a financial year including information regarding the number of notifications made to the Register of Critical Infrastructure Act, directions made under Ministerial Direction powers, the declaration of critical infrastructure assets by the Minister and the enforcement of SoCI. It is proposed that this will be expanded to also include information on:

- the number of annual reports provided under the risk management program;
- the number of cyber incidents reported under the mandatory cyber reporting obligation;
- the number of systems of national significance required to undertake incident response plans, provision of telemetry, vulnerability assessment and cyber security exercise;
- the number of Ministerial authorisations for all aspects of the Government Assistance measures; and
- the number of systems of national significance declared.

3.3. Option Three – No legislative change, achieve improvements to critical infrastructure resilience with voluntary engagement through the Trusted Information Sharing Network and publishing additional guidance alongside the updated Critical Infrastructure Resilience Strategy

The third option focusses on the additional government resources, outlined under Option Two, to enhance engagement on all hazards resilience for critical infrastructure through refreshing the TISN and re-writing the *Critical Infrastructure Resilience Strategy* to identify and provide guidance to Australia's critical infrastructure. This could occur without legislative reform.

Greater engagement with industry would be undertaken through the TISN sector groups as outlined above, noting that industry engagement would continue to be on a voluntary basis. This option would involve a voluntary version of the Positive Security Obligations, Enhanced Cyber Security Obligation and Government Assistance outlined within Option Two. Industry would be encouraged to work with the Government to uplift security against all-hazards and accept Government Assistance where necessary.

However, this option will have limited effectiveness without the support of legislative change. Enforcement under legislation provides a greater degree of assurance to the Government that national security risks are being managed, not just considered. The benefits associated with the additional resources will be restricted as it will be at the discretion of industry to inform the Government of problems and vulnerabilities within critical infrastructure networks. The interconnected nature of these networks also means that any information provided by industry would be incomplete if all assets within a supply chain did not participate.

Entities could be encouraged to report to the Register of Critical Infrastructure. However, this would be reliant on the voluntary provision of information and would therefore likely be incomplete. Further, the Government would have limited scope to utilise this information to better protect these assets without legislative change. Given the interdependent nature of Australia's critical infrastructure, weaknesses in one critical asset could have cascading consequences across sectors.

Current TISN members tend to have a higher level of security and resilience maturity, and this option is likely to further widen the gap between those organisations, and organisations that do not place a high value on resilience beyond commercial imperatives. It is likely that the more mature entities in each sector would engage, but that those entities currently lacking a mature security posture would continue in this posture.

4. RIS QUESTION FOUR: WHAT IS THE LIKELY NET BENEFIT OF EACH OPTION?

4.1. Option One - No regulatory change or enhanced compliance (status quo)

Maintaining the status quo will mean that the Government is unable to provide support and direction to critical infrastructure owners and operators on managing security risks in a timely manner. While organisations likely already consider threats to business operations and utilise security standards as a result of existing frameworks, the level of security is not sufficiently robust across all *critical infrastructure sector*s.

Some critical infrastructure owners and operators may take steps to address risks (such as improving cyber security standards) irrespective of any regulatory change. The benefit of no regulatory change is that owners and operators have the flexibility to address these challenges as they see fit. However,

these steps are generally ad-hoc, influenced by commerciality and either not consistent, or limited to a specific *critical infrastructure sector*.

This option would have the least upfront impost on business given there would be no requirement to uplift security practices. Given existing challenges with COVID-19 this may offer short term benefits to industry. The additional regulatory burden to business, community organisations and individuals under Option One will be nil as no regulatory obligations would be introduced above those that already exist. However, the potential costs of a significant disruption to *critical infrastructure asset*s could be catastrophic to Australia's social and economic stability, defence and national security.

The cost of inaction

Synergy Group, undertook high level economic modelling to determine the costs of inaction without the reforms being introduced. The costs of inaction was quantified by the maximum potential cost of operability disruption to 10% of each of the *critical infrastructure sector*s for a single week.

Uncertainty around the likelihood and severity of all hazards makes it almost impossible to know what the costs of inaction would be. However, to give a sense of the magnitude of the cost of inaction on other critical infrastructure sectors and the broader Australian economy, an operability disruption of 10 per cent has been modelled for each critical infrastructure sector. The possible costs of this scenario for each sector for a single week is estimated at:

- $2.4 billion for the Energy Sector
- $3.0 billion for the Financial Services and Market Sector
- $0.9 billion for the Communications Sector
- $1.0 billion for the Data Storage and Processing Sector
- $1.6 billion for the Higher Education and Research Sector
- $0.7 billion for the Food and Grocery Sector
- $0.6 billion for the Health Care and Medical Sector
- $0.06 billion for the Space Technology Sector
- $1.2 billion for the Transport Sector
- $0.2 billion for the Water and Sewerage Sector

These costs represent the maximum possible cost of inaction if an incident occurred causing a disruption to 10% of a *critical infrastructure sector* for a single week, with smaller incidents likely to cost less. These costs take into account the flow on impacts to other critical infrastructure areas and the broader Australian economy. These costs have not been tested with industry.

The Defence Industry Sector is currently regulated by the Defence Industry Security Program and therefore is unlikely to experience costs of inaction as they are already governed by significant Government oversight preventing significant hazards from having cascading impacts.

Cost assumptions

The cost of the shock is estimated by:

- multiplying total output of the relevant sector by 1/52 to determine the output per week of the sector;
- this figure is then multiplied by 10% to determine the impact – or loss of output – from a disruption to 10% of the critical sector per year.

For example, if the energy *critical infrastructure sector* suffered a 10% operability shock it would imply that Australia's energy *critical infrastructure sector* is only operating at 90% of its ordinary productivity level. A 10% operability shock within the energy sector could occur through a number of

cyber failings or incidents within the energy sector. For example, a 10% operability shock could occur if a supplier of critical SCADA equipment was subject to a cyber incident which impacted multiple SCADA systems across a number of critical energy assets in turn causing the failure of those assets. This in turn would affect the availability of energy causing cascading and compounding disruptions across all the *critical infrastructure sector*s dependant on energy, and the broader Australian economy.

A 10% operability shock within the transport sector could occur if the control centre of the organisation was subject to a weather event resulting in the shutdown of their control centre until alternative arrangements for their operation of the entity could be arranged. This would have significant flow on affects for other *critical infrastructure sector*s such as the food and grocery sector and liquid fuels sub-sector which both rely heavily on the transport sector for transportation of goods from one part of the country to another.

An operability shock of 10% has been employed as it is unlikely that within any *critical infrastructure sector* there will be an entity with a greater than 10% monopoly on the operations of the sector. Therefore, if an entity were disrupted, it is unlikely to have a greater than 10% disruption to the sector.

These costs are indicative. It is difficult to determine the exact extent of the cost of inaction due to the complex, interrelated nature of the *critical infrastructure sector*s and the potential cascading impacts disruptions could have on other *critical infrastructure sector*s and the broader social and economic stability, defence and national security of Australia.

Without proper safeguards across Australia's *critical infrastructure sector*s, hazards may cause long lasting and far reaching consequences.

Benefits	Costs and Limitations
• Affords owners and operators greater flexibility to address risks to critical infrastructure • No upfront or ongoing compliance costs to industry to uplift resilience	• Could have significant flow on effects to the broader Australian economy if a significant hazard were to occur in a critical infrastructure sector. • Does not provide direction and support for owners and operators and leaves industry exposed to a greater risk of all hazard threats • Does not address concerns raised by industry requesting guidance from Government • Unlikely to result in widespread changes in business behaviour or increased security of critical infrastructure and subsequently will not provide the Government greater assurance that risks are being appropriately managed

4.2. Option Two – Legislative change, a compliance and assurance capability

This section provides the costs and benefits of each element of the reforms as described in Question 3. These costs have not been consulted with industry to date. Instead, they have been developed

internally with the assistance of both consultants with subject matter expertise and the Australian Cyber Security Centre for the cyber related elements of the reforms, and build on costings developed prior the SOCI being enacted in 2018.

The maximum aggregated, annual costs to industry as a result of the Register of Critical Infrastructure Assets and the mandatory cyber reporting are below if all critical infrastructure assets were required to comply with these obligations.

Average annual regulatory costs ($ million)				
	Industry	Community	Individuals	Total
Cost	$2.19	-	-	$2.19

Note: the aggregated table does not include the Enhanced Cyber Security Obligations or the Ministerial Directions power. These elements of the reforms do not require ongoing industry obligations and are upon request. Providing aggregate, average annual costs of these elements would likely mislead stakeholders. Instead, the below numbers represent individual costs to entities if directed by Government:

- **ECSO** (applicable only to SoNS):

Incident response plans – maximum annual compliance burden $28,091.30 for a single SoNS assuming annual requirements.
Telemetry - maximum annual compliance burden $81,250 for a single medium SoNS and $361,250 for a single large SoNS assuming annual requirements.
Vulnerability assessments - maximum annual compliance burden $46,875 for a single medium SoNS and $117,375 for a large SoNS assuming annual requirements.
Cyber Security exercises - maximum annual compliance burden $61,425 for a single SoNS assuming annual requirements.

- **Ministerial Directions** (applicable to all *critical infrastructure sector* assets):

Scenario 1 – annual compliance burden for this scenario is estimated at $4,999 on average per entity assuming the direction power will be used once every three years.
Scenario 2 - annual compliance burden for this scenario is estimated at $280,741 on average per entity assuming the direction power will be used once every three years.
Scenario 3 - annual compliance burden for this scenario is estimated at $279,541 on average per entity assuming the direction power will be used once every three years.

Option Two of the Regulation Impact Statement is likely to have the highest overall net benefit. Recalibrating industry's risk posture to safeguard against all hazard threats will make strong and effective security practices part of doing business in Australia. It will improve industry resilience, creating a more secure and reliable market for both regulated and non-regulated sectors, ultimately decreasing the impacts of potential disruptions to critical infrastructure.

This option aligns with industry and community expectations for the Government to protect Australia's critical infrastructure, as well as safeguard Australia's social and economic stability, defence and national security more broadly. Furthermore, clear uplift in all hazard mitigation standards across critical infrastructure will provide the Government, industry and consumers with greater confidence in the resilience of Australia's critical infrastructure providers and the essential services they rely on.

4.2.1 Positive Security Obligations

The Positive Security Obligations (PSO) will contain three elements:

1. The Critical Infrastructure Risk Management Program;
2. Register of Critical infrastructure assets; and
3. Notification of cyber security incidents.

Government acknowledges there will be costs and benefits to *critical infrastructure assets* through the introduction of the PSO. This RIS includes the qualitative impact of the (1) risk management programs, and the qualitative and quantitative impact of the (2) register of *critical infrastructure asset*s and (3) notification of cyber incidents. The quantitative impact of the (1) risk management program will be developed in a future RIS(s) when the sector specific obligations are further developed and costs and benefits can be more accurately identified with industry.

1. The Critical Infrastructure Risk Management Programs

Costs

There is a risk of duplicating existing regulations across states and territories. The Government will minimise the risk of regulatory duplication and the subsequent regulatory impact on business by engaging with industry to co-design the sector specific rules for the Risk Management Program. This will help to ensure:

- Government actively considers offsetting the potential regulatory burden experienced by industry
- Industry has greater certainty about how the reforms impact them, focusing specifically on the risks to their business, and how they can best comply with the proposed regulations, avoiding unnecessary costs as a result of misinterpretation.
- The Government better understands the potential regulatory overlap as a result of the reforms, ensuring that duplication is minimised as much as possible.
- That existing regulations, frameworks and guidelines are leveraged to minimise regulatory cost wherever possible.
- There will be greater continuity for foreign investors regarding their security obligations and understanding that the Positive Security Obligations provide a level playing field for all *critical infrastructure asset*s regardless of ownership.
- That Government leverages existing regulations to avoid supressing innovation.

It is expected that some sectors will already have existing measures in place to manage all hazards and as a result there will only be a small regulatory impost. The costs associated with additional regulation will be further explored in future RIS(s), where detailed economic modelling will be undertaken alongside industry and state and territory governments.

Benefits

Introducing the risk management program will ensure that industry has the necessary direction and guidance to address all hazard risks to *critical infrastructure asset*s where those risks are not currently managed, or are not addressed consistently across *critical infrastructure sector*s.

A positive externality of the reforms is that the uplift of one entity's security against all hazards risks will increase the resilience of downstream entities. For example:

- The sensitive data created and held within the health sector needs to be protected by both the sector and the data centres that may store such information. If not properly protected and stored, the content of the data could have significant security ramifications including additional burden of customer reporting as a result of a data breach, reputational damage and legal penalties.
- Lax personnel security within a telecommunications company can result in weaknesses being exploited within a network and can impact a range of *critical infrastructure asset*s that rely on telecommunication services to function. This could include, freight and passenger rail and electricity transmission networks, having flow on affects to all areas of Australia.

These externalities can be small in size, but more often than not the depth of interconnectivity between *critical infrastructure asset*s mean that consequences of failings within *critical infrastructure sector*s can be severe.

Another externality is created through an increase in job opportunities, and long term employment for households. In implementing the proposed regulation, opportunities exist for the Australian industries that specialise in products and services that can assist *critical infrastructure asset*s in meeting the objectives of the proposed reforms. For example, business process improvements, risk mitigation and support, and operational resilience.

The industries most likely to benefit from the new regime are the public administration and safety sector, cyber security sector, and professional, scientific and technical services. For example, an uplift in Australia's cyber security will build Australia's cyber security industry and bolster the technical skills required to support the nation's growing digital economy. The quantitative benefits of such externalities and the possible costs of resulting externalities, such as shortages of staff will be further explored in future RIS(s).

Households will also benefit through an increase in the resilience of Australia's critical infrastructure which reduces the likelihood of significant disruptions to essential services. Increased resilience creates stability in household income due to industrial production resilience, security, and stability which in turn promotes job growth and job security. Further benefits would also be derived from employment opportunities in the provision of goods and services to ensure *critical infrastructure sector*s achieve regulatory compliance.

This option will support the Government to shape a market that considers all-hazards risks. The risk management program will ensure that the Government can drive industry-wide management of risks in the absence of market drivers, avoiding any market imbalances that currently result from the case-by-case application of security controls through the FATA. This option also provides certainty and consistency for the critical infrastructure owners and operators by creating a level playing field for both domestic and foreign investors.

While there will continue to be a need for case-by-case assessments of investment applications, the PSO will reduce the existing burden on the foreign investment review framework to manage risks. Currently, the Department advises the Department of Treasury on conditions that it considers should be imposed on critical infrastructure foreign investment. Through the proposed SoCI reforms there is the ability to have conditions already in place for *critical infrastructure assets* to manage risk. Previously, the CIC has made recommendations to the Department of Treasury that certain foreign businesses acquiring critical infrastructure in Australia under the FATA take certain steps to manage the security of data. Through the proposed SoCI reforms, this type of recommendation may no longer be necessary as the Act will provide the opportunity to address this risk through ongoing obligations within the risk management program. It is expected that this will streamline consideration of lower risk acquisitions (under current and future foreign investment settings) providing benefits for foreign investors, and enable Government resources to be focused on managing higher risk investments.

The co-design of sector specific rules in early 2021 with industry will help minimise innovation from being stifled as a result of increased regulations. By co-designing the specific rules for the Risk Management Program*,* industry will be able to guide the development and design of the rules, presenting opportunities for industry to source innovative solutions to uplifting the security of critical infrastructure.

2. Register of Critical infrastructure assets

Costs

In total, it is expected that no more than 1,700 entities will fall within the definition of *critical infrastructure asset*s across the 11 sectors. Currently, 167 entities already report to the Register of *Critical infrastructure asset*s and their regulatory burden for this obligation will not change as a result of the introduction of the proposed reforms. The remaining 1,500 or so entities that do not currently report to the Register of *Critical infrastructure asset*s, will experience an increase in regulatory burden if that obligation is switched on. This will be done through the Minister declaring within the sector specific rules which critical infrastructure assets will be subject to the reporting requirements.

The largest regulatory cost burden for entities lies in obtaining and inputting information about legal and beneficial ownership, given that most entities are likely to have multiple legal and beneficial owners. Many of the costing assumptions have been informed by those that were provided in the SoCI 2018 Explanatory memorandum when the register was first introduced.

The following method was used to calculate the annual cost of complying with the register for an average entity. This method is in line with Office of Best Practice Regulation guidance.

Annual cost for entity = (time required to report * hourly cost ($41.74)* wage multiplier (1.75)) * (times performed annually * number of staff)

Cost description	Cost
Upfront cost for a single entity (Year 1)	$4,041.80
Annual administrative cost for a single entity	$259.59
10 year cost for a single entity	$6,378.10
Aggregated cost for all Critical Infrastructure assets (over 10 years)	$9,567,135.97

*Maximum cost assuming the obligation is applied to all assets

Costing assumptions

- Each *critical infrastructure asset* spends 55 hours providing the operational, initial interest and control information and then 3.6 hours on average updating interest and control information annually.
- The average period that a direct interest holder holds its interest in an asset is 4.3 years.[14] Therefore, in the ten-year costing timeframe, reporting a change in a direct interest holder is assumed to happen 2.3 times.
- The average period in which an 'other entity' holds an interest in a direct interest holder is 2.5 years.[15] Therefore, in the 10 year costing timeframe, reporting a change in details of an 'other entity' is assumed to happen four times.
- Hourly rate is $73.05 as per OBPR guidance. It is assumed that there will be no legal expertise required to complete the register on the online portal and guidance provided by the CIC will assist entities in understanding their obligations.
- Interest and control information includes direct interest holders' details, name and citizenship details of board members, ownership thresholds and voting rights for board members, and access rights and privileges to operational systems and corporate network for board members.

The CIC has existing guidance that it will update to assist new critical infrastructure assets to understand their obligations. This guidance is expected to be provided to all impacted entities through the TISN and will be published on the CIC's website. The upfront labour cost is unlikely to vary across different sized organisation as understanding the obligation and reporting will be the same for

[14] SoCI 2018 Explanatory Memorandum
[15] Ibid

all business regardless of their size. Furthermore, the size of the entity does not necessarily determine the complexity of the organisational or ownership structure, therefore costings have not been differentiated based on size. The costs will decrease if it is found that there are existing adequate reporting obligations that sectors are already subject too.

The Government IT solution for the Register already exists and as such, minimal costs to Government are expected to result from the expansion of the register to capture all newly defined *critical infrastructure asset*s.

Benefits

The benefit of the Register is that it provides a single comprehensive resource of information on legal and beneficial ownership and control of *critical infrastructure asset*s. Information from the Register would also be able to be shared with states and territories in prescribed circumstances to assist in their understanding of *critical infrastructure asset*s in their jurisdiction.

The increased scope of the Register enables 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 CIC to:

- assess ultimate ownership of assets and influences by particular individuals or companies,
- analyse interdependencies among *critical infrastructure asset*s and sectors, and
- identify commonalities in services being used by *critical infrastructure asset*s, such as shared IT service providers or shared control systems.

3. ***Notification of cyber security incidents***

Costs

Cost description	**Cost**
Upfront cost for a single entity (Year 1)	$237.41
Annual administrative cost for a single entity (small)	$219.15
Annual administrative cost for a single entity (medium)	$657.45
Annual administrative cost for a single entity (large)	$1,095.75
10 year cost for a single entity (small)	$2,428.91
10 year cost for a single entity (medium)	$6,811.91
10 year cost for a single entity (large)	$11,194.91
Aggregated cost for all 1,700 *critical infrastructure assets* (over 10 years)	$12,325,361.25

It is unlikely that the quantitative regulatory burden experience by organisations will vary between the two tiers of cyber reporting defined in section 3, as the same response is required from the affected entity just within different time frames. It is recognised however that entities may have to reprioritise work to meet the differing deadlines and this may have flow on costs to their organisation, such as the postponement of other work or a delay in the provision of services. These costs are difficult to quantify but should be acknowledged when considering costs of the obligation. These costs have been reviewed by the Australian Cyber Security Centre.

Cost Assumptions:

- The scaled up rate of $73.05 per hour has been used to reflect OBPR guidance.
- Approximately 1,700 businesses may be subject to the obligation. Approximately 340 small businesses, 850 medium business, and 510 large businesses.

- The ACSC currently sees 1,268 cyber reports a year (from 2019/2020) under their voluntary reporting scheme or approximately 2.5 reports a year from large businesses.[16] This number is expected to increase if these reforms are implemented and reporting requirements are mandated for all critical infrastructure assets.
- No legal expertise are expected to be required to understand the obligations to report or to report if there is a cyber incident.

Upfront

- One member per business would dedicate approximately 3 hours of their time to become aware of their obligations to report a cyber security incident to the Australian Cyber Security Centre. This would include one hour for an individual to read guidance documents that will be provided by CIC on an entity's obligations, an estimated two hours dedicated to creating standard operating procedure documentation for the organisation to adhere to their obligations, and a final 15 minutes for an individual to disseminate the information throughout their organisation (likely a business wide email informing employees of their obligations).
- The upfront labour cost is unlikely to vary across different sized organisation as understanding the obligation will be the same for all business regardless of their size.

Ongoing

- One member per business would dedicate approximately 3 hours of their time once a year to report a cyber security incident to the Australian Cyber Security Centre. This would involve a member of an organisation becoming aware of a cyber security incident, identifying the key components of the incident, such as what type of incident it was and how it occurred (i.e. through a phishing email) and then summarising the incident in an email or through a phone call to the Australian Cyber Security Centre.
- Small businesses will experience approximately one cyber incident annually significant enough to require being reported to the Australian Cyber Security Centre.
- Medium businesses will experience approximately three cyber incident annually significant enough to require being reported to the Australian Cyber Security Centre.
- Large businesses will experience approximately five cyber incident annually significant enough to require being reported to the Australian Cyber Security Centre.
- This assumes an annual total of 340 cyber reports annually across all small organisations, 2,550 across all medium organisations and 2,550 across all large organisations – or a total of 5,440 reports annually across all critical infrastructure assets. Given the ACSC experienced 1,268 cyber reports in 2018/19, 5,440 reports assumes that once the reforms are implemented there will be a marked increase.

Benefits

The objective of this part of the reforms is to facilitate the development of an aggregated threat picture and comprehensive understanding of cyber security risks to *critical infrastructure asset*s 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 Cyber Enhanced Situational Awareness and Response package (CESAR).

[16] ACSC Annual Cyber Threat Report July 2019 to June 2020, <https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf>

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. This will ultimately reduce the risks of security incidents by ensuring industry and Government have the most up to date visibility of threats within the cyber domain. It will address the lack of Government visibility addressed within section 1.

4.2.2. Enhanced Cyber Security Obligations

In identifying the costs and benefits of the Enhanced Cyber Security Obligations, PricewaterhouseCoopers Consulting (PwC) were engaged. PwC have significant cyber security experience which informed the underlying costing assumptions including the skills required and the industry rates. The Australian Cyber Security Centre and the Office of the Chief Economist from the Department, also undertook a high level review of the approach taken by PwC.

Costs

The regulatory costs of imposing Enhanced Cyber Security Obligations would vary widely depending on the scope of the obligations and the individual circumstances of the entity subject to the obligations. The obligations will only be enlivened on request. 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 in an effort to reduce regulatory burden and offset potential costs. However, there may be instances where entities are unwilling or unable to voluntarily cooperate and the Enhanced Cyber Security Obligations are necessary. Government will seek to provide assistance wherever possible in *systems of national significance* complying with these obligations.

It is expected that there would be approximately 40 SoNS declared by the Minister.

1. Incident response plan

Incident response plans are designed to strengthen a business' preparedness for a cyber security breach.

Cost description	**Cost**
Upfront cost for a single entity (Year 1)	$25,538 - $76,613
Annual administrative cost for a single entity	$10,215 - $20,430

Cost assumptions:

- Although many SoNS are likely to already have an existing incident response plan that can be provided to the CIC, this analysis assumes each SoNS will need to at least update their incident response plan to comply with the obligation.
- Three people within an organisation would be required to develop an incident response plan (a security operations lead at $250 an hour, a security operations analyst at $188 an hour and a head of security at $486 an hour).
- All entities will have the same upfront costs to either develop an incident response plan or update an existing plan.
- It is expected that it will take between 1-3 weeks to develop an incident response plan with one week being the low scenario and three weeks being the high scenario. The low and high scenario will depend on the level of an entity’s existing maturity.
- To maintain and update an incident response plan annually, it would require the same three individuals from the organisation.

- It would take between 2 and 4 days for an entity to update their response plan with 2 days being the low scenario and 4 days being the high scenario.
- Due to the nature of a SoNS it is not expected that a small organisation would be declared a SoNS.

2. Provision of telemetry

An organisation's ability to detect and respond to a cyber incident depends on having visibility across their technology environment. This visibility is provided in the form of telemetry (often referred to as system logs) that are usually aggregated into a centralised security operations capability. Where an organisation does not have the capability to provide telemetry, these services will be provided by the Government.

Cost description	**Cost**
Upfront cost for a single medium entity (Year 1)	$18,750
Upfront cost for a single large entity (Year 1)	$18,750
Annual administrative cost for a single medium entity	$49,375 - $79,375
Annual administrative cost for a single large entity	$209,375 - $359,375

Cost assumptions

- Upfront costs include a security operations lead at $250 an hour for two weeks being required to set up the capability to transmit telemetry.
- Ongoing costs include the cost of a security operations lead at $250 an hour for one week being required for the ongoing reporting and an annual cost for technology deployment.
- Upfront costs of technology deployment: an entity may opt to choose their own technology to provide access. Sensors can cost anywhere between $20-35 per/host/year for both the technology and analysis. The size of the organisation will drive cost in this regard as well as the degree of coverage. For a medium size organisation (less than 2,000 hosts) it would cost $40,500-$70,000 per annum and for a large organisation (over 10,000 hosts) $200,000-$350,000 per annum. The low range assumes $40,500 and $200,000 and the high range assumes $70,000 and $350,000. We assume 50 per cent of all organisations would uptake this cost.
- Reporting costs for the compilation and transmission of telemetry to be shared with Government: this consists of an upfront cost to set up the reporting procedures in place in the first year and ongoing reporting costs on annual basis. It is estimated that the initial upfront process would take two weeks with the annual reporting to be one week of full time work for a security operations lead.
- PwC has made these assumptions based on their own experiences and desktop research.
- Due to the nature of a *systems of national significance* it is not expected that a small organisation would be declared a *system of national significance*.

3. Vulnerability assessment

Conducting a vulnerability assessment in relation to a specific computer system or network can inform the effectiveness of the cyber security arrangements in place. The goal is to identify as many security vulnerabilities as possible.

If a vulnerability assessment is required to be undertaken by an organisation there will be consultation between Government and the entity to determine whether they have the capability to undertake this. If the Secretary has reasonable grounds to believe that an entity would not be capable of complying with a request or has not complied with request in the past than the Government may offer assistance to provide the service on behalf of the directed entity.

If an entity did not already undertake vulnerability assessments as a matter of course, the entity could procure software or engage third party contractors to undertake vulnerability assessments. The cost of a vulnerability assessment will vary depending on the size of the network, speed, frequency and experience of the tester. Costs to outsource this work if the skills are not held internally are accounted for in these costings.

Cost description	Cost
Annual cost for a single medium entity	$46,875
Annual cost for a single large entity	$117,375

Cost assumptions

- There are no upfront costs associated with conducting a vulnerability assessment.
- The costs of conducting a vulnerability assessment differs based on the size of an organisation's network as well as their technology environment. This has significant implications on duration and resourcing required. For the purpose of this analysis, two main components have been factored:
    - Size of organisation: This refers to the number of systems on a network. We assume a vulnerability assessment for an organisation with a medium network would require one security operations lead, where a large network would require two additional security operations analyst for support. This is due to the additional time it takes for vulnerability scans to run, and for the results to be manually interpreted. We assume the assessment would be done for subset of systems/networks that are the highest risk/criticality for the organisation, rather than every system on the network.
    - Technology environment: There are significant differences in how vulnerabilities can be assessed in IT versus OT networks. OT systems necessitate a more manual approach due to the risks of running automated scans, and this is more time consuming and complex. OT systems can often be in remote locations which also increases the time for an assessment. We have assumed two thirds of SoNS have a notable amount of OT in their environment (e.g. multiple critical OT based systems), based on our experience working across critical infrastructure sectors.
- We assume that each organisation only conducts one vulnerability assessment per annum.
- The annual administrative costs for a medium organisation are calculated assuming that a single security operations lead at $250 per hour would require one week to conduct a vulnerability assessment on their IT system, and 4 weeks on their IT/OT systems.
- The annual administrative costs for a large organisation are calculated assuming that one security operations lead at $250 per hour and two security operations analysts at $188 per hour would require one week to conduct a vulnerability assessment on their IT system, and 4 weeks on their IT/OT systems.
- Due to the nature of a *systems of national significance* it is not expected that a small organisation would be declared a *system of national significance*.

4. Cyber security exercise

Conducting a cyber security exercise is an important activity for an organisation to test and improve their cyber resilience. A tabletop exercise (paper based walkthrough) and a functional exercise (end-to-end simulation) has been costed. The functional exercise is significantly more detailed and resource intensive.

Cost description	Cost
Annual cost for a single entity	$30,488 - $61,425

Cost assumptions

- It is not expected that the cost of conducting a cyber security exercise would differ between a medium and a large organisation.
- There are no upfront costs associated with conducting a cyber security exercise.
- Preparing a tabletop cyber security exercise will require one week of work from a security operation lead at $250 per hour and a security operations analyst at $188 per hour.
- One cyber security exercise is undertaken annually.
- Undertaking a tabletop cyber security exercise will require five individuals from across an organisation (security, legal, operations, HR and public affairs) to partake in an exercise expected to take 1.5 days' worth of work. This includes a half day for the event and another day to write-up the lessons learnt.
- Undertaking a functional cyber security exercise will require six individuals from across an organisation (security, legal, operations, HR and public affairs) to partake in an exercise expected to take 4 days' worth of work, this includes 1 day for reporting on lessons learned. The functional exercise is more resource intensive and provides organisations to realistically test their cyber resilience and response processes.

Benefits

The benefits of the Enhanced Cyber Security Obligations align with those that will be experienced through the Positive Security Obligations (positive industry and household externalities; aligning industry and community expectations of the Government; and lifting the resilience of Australia's critical infrastructure businesses).

The Enhanced Cyber Security Obligations will also ensure that the Government has the necessary powers to increase cyber security preparedness for Australia's most critical infrastructure, actively protecting their cyber networks and having plans in place to prevent, react to and mitigate cyber-attacks which are posing increasing threats. Specifically:

- Incident response plans will strengthen a business' preparedness for a cyber security breach, driving an uplift in security and resilience.
- Telemetry will improve an organisation's ability to detect and respond to a cyber incident by providing visibility across their technology environment. This measure will improve situational awareness across Government which can in-turn be used to inform industry on possible threats to improve preparedness, reducing the likelihood of a cyber incident.
- Conducting a vulnerability assessment in relation to a specific computer system or network will seek to inform the effectiveness of the cyber security arrangements in place for an entity.
- Conducting cyber security exercises will form an important activity for an organisation to test and improve their cyber resilience.

Without this power, the Government would only be able to request that critical infrastructure owners mitigate their own cyber risks, and rely on mutual interest to ensure cyber risks are addressed. The four components of the Enhanced Cyber Security Obligations each look to reduce the risks of cyber security incidents occurring.

These reforms align with business and community expectations for Government action to safeguard the continued supply of essential services all Australians rely upon. Through consultation it was highlighted that the Australian public looks to both the Government and critical infrastructure providers to secure the delivery of essential services. These reforms ensure that the Government is

able to work alongside industry to provide assistance in emergencies and is able to proactively secure Australia's critical infrastructure.

4.2.3. Government Assistance

The Government Assistance measure would only occur in the event of a cyber-crime being committed and as such quantification of regulation costs have not be conducted. This is because those costs arising from non-compliance, or a suspicion of non-compliance, are excluded from the Government's Regulatory Burden Measurement framework.

Costs

The regulatory costs of imposing Government Assistance would vary widely depending on the scope of the request (whether it be an information gathering request, an action direction or an intervention direction) and the individual circumstances of the entity subject to the assistance.

There is a minor risk Government intervention leads to adverse, unintended consequences which may occur as a result of Government not understanding a critical infrastructure assets control systems. To mitigate this risk, only suitably qualified cyber specialists will be engaged and ongoing consultation will be maintained between Government and the critical infrastructure entity to ensure that any actions are informed by specialist advice from the entity. Furthermore, extensive consultation will be conducted with the affected entity prior to any Government action providing further safeguards against damage occur to an asset as a result of Government Assistance measures.

There are also potential moral hazards that may arise from the use of the Government Assistance measures where Government steps in to provide assistance during a cyber-security incident. For example, entities may engage in riskier behaviour and may not address cyber security vulnerabilities or implement response plans to cyber security incidents if they believe that the Government may step in and assistance, thereby removing the burden and responsibility from industry and placing the onus on Government. The risk of moral hazards can be reduced through extensive industry-Government engagement where Government reiterates that these powers are intended purely as a last resort method only for use in extreme circumstance. The mandatory requirement for *critical infrastructure assets* to also implement risk management programs, and the associated penalties for non-compliance, will also ensure that *critical infrastructure assets* are proactively protecting themselves against potential significant cyber incidents.

Benefits

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.

Introducing the Government Assistance measure will ensure the Government has the necessary powers to address cyber risks to critical infrastructure where these cannot, or will not, be managed by the entity affected. Without this power, the Government would only be able to request assistance from critical infrastructure owners to mitigate cyber risks, and rely on mutual interest to ensure the cyber risk is addressed.

This measure will also provide *critical infrastructure asset*s with timely support from Government where needed. Without this measure, entities may be hesitant to accept voluntary assistance from

Government without a clear directive to do so. Where an entity is subject to a cyber-attack there is often a need to respond in a timely manner as any delay can increase consequences exponentially.

4.2.4. Expansion of Ministerial Direction

The regulatory costs of imposing a Ministerial direction would vary widely depending on the scope of the direction and the individual circumstances of the entity subject to the direction. In assessing the expected costs to industry as a result of the expansion of the Ministerial Directions powers, we have applied the same methodology to that which was used in the SoCI 2018 Regulation Impact Statement. While the Ministerial Directions powers will be expanded to all new *critical infrastructure sector*s, it is not expected that the costs would deviate significantly from the original sector cost estimates provided in the SoCI 2018 Regulatory Impact Statement.

In the SoCI 2018 Regulatory Impact Statement, four scenarios were modelled for the original sectors captured under SoCI (electricity generation, electricity transmission/ distribution, gas processing/storage, gas transmission/ distribution, ports and water) with breakdowns provided across small, medium and large organisation. Note: this Regulation Impact Assessment costs three of these scenarios given one of the scenarios previously costed is no longer relevant.

Costs

Scenario 1 – Direction requiring a business to limit any offshore access to its industrial control systems unless where approved by Government.

a. Assuming the Direction power will be used once every three years (frequency of 3.33 across the 10 year costing timeframe) the annual compliance burden for this scenario is estimated at $4,999 on average per sector.
b. The annual cost of a single occurrence of the ministerial direction power over a ten year period, averaged for each sector is estimated at $86,875 for a small business, $81,353 for a medium business and $77,672 for a large business.

Scenario 2 – A direction preventing a business from outsourcing the operations of its core network to certain low-cost, low-quality providers.

a. Assuming the Direction power will be used once every three years (frequency of 3.33 across the 10 year costing timeframe) the annual compliance burden for this scenario is estimated at $280,741 on average per sector.
b. The annual cost of a single occurrence of the ministerial direction power over a ten year period, averaged for each sector is estimated at $1,385,499 for a small business, $4,020,916 for medium a business and $6,656,332 for a large business.

Scenario 3 – A direction preventing a business from sourcing core operational systems technology from certain low-cost, low-quality providers.

a. Assuming the Direction power will be used once every three years (frequency of 3.33 across the 10 year costing timeframe) the annual compliance burden for this scenario is estimated at $279,541 on average per sector.
b. The annual cost of a single occurrence of the ministerial direction power over a ten year period, averaged for each sector is estimated at $1,419,972 for a small business, $3,514,742 for a medium business and $7,096,694 for a large business.

Note: the ministerial directions power has not been used since introduction in 2018. As such, (b) the annual cost of a single occurrence of the ministerial direction power over a ten year period for each sector and business size category is illustrative only. Assuming a ministerial direction is used (a) once

every 3 years is considered more realistic and subsequently more representative of the likely costs to industry.

Cost assumptions:

- The following method was used to calculate the annual cost of complying with the register for an average entity. This method is in line with Office of Best Practice Regulation guidance.
    - **Regulatory burden = (time required to report * hourly cost ($41.74)* wage multiplier (1.75)) * (times performed annually * number of staff)**
    - Where relevant, the time required to report has been informed by a complexity multiplier, and/or a SCADA expertise multiplier and/or an industry multiplier to account for different levels of complexity across sectors. The averages have been used to inform costs.
- The sectors (electricity generation, electricity transmission/ distribution, gas processing/storage, gas transmission/ distribution, ports and water) that were costed in the SoCI 2018 Explanatory Memorandum provide a suitable analogue for all *critical infrastructure sector*s.
- Independent compliance audits, staff training, procurement related to SCADA systems or new communications infrastructure providers, costs of breaking existing contracts and software updates and maintenance have been considered in costings.

a. Ministerial direction is used every 3 years

- The ministerial directions power will be used once every three years (resulting in a frequency of 3.33 across the 10 year costing timeframe).
- Each of the three scenarios is assigned an equal probability of occurring (33% each).
- Within each of the three scenarios, the 33% probability is split between small, medium, large entities types.
- A medium and large sized entity is twice as likely to be affected by a Ministerial Direction power direction compared to a small sized entity.

b. Ministerial direction for each sector and business size once every 10 years

- The costs for small, medium and large businesses have been determined using the modelling work undertaken in the 2018 SoCI Regulation Impact Statement and averaging the costs of all sectors for a small, medium or large business.

The Minister's use of the directions power may change foreign investors' perceptions of sovereign risk in Australia if it is considered that the directions power is being abused. This would have a significant impact on the Australian economy which is highly dependent on foreign capital which is needed to grow the economy, increase productivity and living standards, and to create jobs. However, the fact that the Ministerial direction power has been in force for the last two years and has not yet been used should alleviate these concerns.

Benefits

The Ministerial directions power was introduced into current SoCI to ensure that the Government had the necessary powers to address national security risks to critical infrastructure where they could not be managed through other mechanisms. Since its introduction, there have been no incidents where the Ministerial directions power has been required.

Without this power, the Government would only be able to request assistance from critical infrastructure owners to mitigate risks, and rely on mutual interest to ensure the risk is addressed. The benefit of the directions power is in instances where assistance is not provided and risks are not mitigated. Subject to the safeguards in issuing a direction, this power allows the Government to ensure that the underlying national security risks are addressed.

As critical infrastructure has become increasingly interconnected over recent years it is important that the Ministerial Direction powers are expanded to include all newly defined *critical infrastructure asset*s.

4.2.5. Voluntary engagement through the Trusted Information Sharing Network (TISN)

Costs

Participation within the TISN will be on a voluntary basis and therefore will not result in a regulatory burden to industry. For those that voluntarily participant, there will likely be a number of events that participants will be invited to join as well as a number of guidance documents and briefing materials provided to industry

Benefits

By complimenting legislative change with revitalising the TISN and the *Critical Infrastructure Resilience Strategy* further cost benefits for industry will be realised. Revitalising the TISN and the *Critical Infrastructure Resilience Strategy* will help to encourage the successful development and implementation of standards, uplifting the overall security of critical infrastructure. However, as engagement with the network and the strategy will be voluntary only those businesses that choose to participate will incur costs. Further, businesses are able to choose to participate in some components of the program and not others as best suits them, only incurring costs associated with their chosen components.

Participants engaging with the revitalisation of the TISN and the *Critical Infrastructure Resilience Strategy* will receive a number of benefits. Through the various components of the program, participants will have access to Government risk information, expertise and advice on the threat environment and managing security risks to their business, targeted threat information and briefings from security agencies, guidance from the Government and fellow industry participants on security practices, and the opportunity to shape the development of industry codes of conduct and standards. Engagement will assist participating owners and operators to make more informed and effective security investment decisions, and assist those operators already subject to existing regulation meet their obligations. Additionally, active engagement in the TISN will be taken into consideration if and when compliance action is required. All of these will benefit participants by supporting improved security outcomes and more efficient practices and standards.

Financial Support

The Government does not intend to offer financial support to critical infrastructure owners and employees in meeting the proposed reforms. However, the Government will use the refreshed TISN engagement mechanism to provide assistance in the way of education and training for critical infrastructure owners and operators to meet the new standards and reporting requirements. The Government also believes that a wide reaching uplift in security across *critical infrastructure sector*s (regardless of regulatory coverage) will provide long term benefits to industry through greater security across their supply chains and greater assurance and clarity around real threats to their assets and appropriate measures to safeguard themselves.

Flow on costs to individuals

Some of the costs experienced by industry through an uplift in all hazard risk management will be passed onto households that consume the critical infrastructure outputs; for example electricity and water. This cost pass-through must be balanced against the resilience benefits for households and businesses, as less significant disruptions will result in greater continuity and resilience of services.

Variability of costs

The costs provided in the Regulation Impact Statement are contingent on a range of variables. These variables include: size and complexity of the entity's operations; which sector/s the entity exists within; entity type; investor and consumer pressure; reputational risk; financial resources; perceived costs and benefits of compliance; understanding of the regulations and level of engagement with the regulations; and the current maturity of an entity and whether they already comply with similar regulations.

Costs to the Government

An engagement focussed, risk based approach to compliance will be taken by Home Affairs which is anticipated to be the primary regulator for most, if not all sectors. Co-design of sector specific rules will occur throughout 2021 with the rules being 'switched on' following a designated grace period. Once the Department has gained greater clarity on the number of entities that will have obligations and the type of specific obligations under the PSO after co-design with industry then the Department will be able to provide quantified costs to Government. These will be provided within future RIS(s) and publicly available through future Budget papers.

The CIC will focus on education and assistance wherever possible with enforcement of compliance only being used where absolutely necessary to mitigate risks. To deliver industry engagement, guidance and compliance there will need to be an investment in specialist knowledge and skills to ensure effective consultation across industry and states and territories.

In the development of the costs to Government, the Department will work closely with central agencies to ensure there is broad agreement to the approach being taken.

Benefits	Costs and Limitations
• Safeguards Australia's social and economic stability, defence and national security by increasing critical infrastructure resilience. • Provides certainty for businesses by setting clear standards for action and creating a level playing field in the Australian market for businesses considered critical infrastructure. • Aligns with business and community expectations for Government action. • Drives improved all hazards supply chain management. • Enables the Government to develop real-time situational awareness from high criticality entities allowing the Government to respond effectively and efficiently to emergencies. • Provides business with access to Government risk information, expertise and advice on the threat environment and managing security risks to their business.	• The regulatory option may impose significant upfront cost on *critical infrastructure assets* and *Systems of National Significance* to comply. This may impact their viability and ability to innovate. • As a result of increased regulation costs to industry, it is expected that some of the costs will be passed onto consumers through increased bills (e.g. electricity, food costs). • This option is expected to have the highest cost to Government as a result of engagement, guidance and compliance measures required as a result of a regulatory approach. • There is a risk that the regulatory obligations imposed on *critical infrastructure assets* and *Systems of National Significance* create unnecessary administrative burden that is not commensurate with the risk. • **PSO:** Mandatory Cyber Reporting – average annual compliance burden of $242.89 per small entity, $681.19 per medium entity, and $1,119.49 per large entity.

• Provides business with guidance from Government and fellow industry participants on security practices.	Register of Critical Infrastructure Assets – average annual compliance burden of $637.81 per entity. • **ECSO:** Incident response plans – maximum annual compliance burden $28,091.30 for a single SoNS assuming annual requirements. Telemetry - maximum annual compliance burden $81,250 for a single medium SoNS and $361,250 for a single large SoNS assuming annual requirements. Vulnerability assessments - maximum annual compliance burden $46,875 for a single medium SoNS and $117,375 for a large SoNS assuming annual requirements. Cyber Security exercises - maximum annual compliance burden $30,488 for a single SoNS assuming annual requirements. • **Ministerial Directions:** Scenario 1 – average annual compliance burden for this scenario is estimated at $4,999 per entity. Scenario 2 – average annual compliance burden for this scenario is estimated at $280,741 per entity. Scenario 3 - annual compliance burden for this scenario is estimated at $279,541 on average per entity.

4.3. Option Three – No legislative change, revitalising the Trusted Information Sharing Network and the Critical Infrastructure Resilience Strategy

Revitalising the TISN alone could have a number of benefits and may assist critical infrastructure owners and operators in responding more effectively to national security risks without imposing additional compliance costs through new regulation. Promoting voluntary action would allow owners and operators to work collaboratively to design and implement industry-led responses, reducing the need for Government intervention.

However, the success of voluntary, non-regulatory measures is contingent on business engagement. While industry engagement is expected to be positive, it will continue to be piecemeal. The lack of legislative reform diminishes the effectiveness of this program due to the lack of enforcement capabilities. The most likely owners and operators to adopt voluntary principles or utilise guidance material are those already acting to mitigate national security risks. Those deterred by the commercial disincentives are less likely to voluntarily take action.

For the TISN to succeed positive industry engagement is vital. This will result in the successful development and implementation of standards and uplifting the overall security posture of critical infrastructure. However, without the support of greater enforcement mechanisms and the proposed legislative security regulatory regime, the Government is not confident that real and sustained security outcomes can be achieved. Without legislative reform, the Government will continue to manage national security risks through the FATA and subsequently not deliver a security uplift for critical infrastructure that is domestically owned and operated.

The cost to industry would be dependent on who within industry voluntarily engages with the TISN and voluntarily uplifts their security through non-regulatory versions of the Positive Security Obligations, Enhanced Cyber Security Obligation, and Government Assistance. It is likely that not all

entities deemed critical infrastructure would participate and therefore the costs to industry in reality would be significantly lower than the cost of making the obligations regulatory. Similarly, the corresponding benefits would also be significantly lower than Option Two.

An increase in resilience in some *critical infrastructure asset*s would provide greater benefits to the security and resilience of Australia's social and economic stability, defence and national security. However, due to the interconnected nature of critical infrastructure a broad uplift across sectors is required to substantially improve the resilience of critical infrastructure, and this is unlikely to occur without regulatory obligations.

Benefits	Costs and Limitations
• Owners and operators have the flexibility to address risks to critical infrastructure • Addresses concerns raised by industry requesting guidance from Government • Reduced need for the Government to intervene • No new regulatory compliance costs for business and the Government	• Costs to industry dependent on level of industry engagement. • Success in meeting the Government objectives of the reform is contingent on industry engagement • Lack of legislative drivers diminishes effectiveness due to lack of enforcement capabilities • Without regulatory obligations providing clear direction, many businesses will lack a clear mandate to uplift all hazards risk management • Those not already utilising guidance material are unlikely to voluntary engage in mitigating identified risks • Continued overreliance on FATA, impacting Australia's investment reputation • The gaps between organisations with high security and resilience maturity and those with low maturity will continue to widen

5. FEEDBACK

This section provides an overview of the Government's public consultation process. This section explains the purpose and objective of the consultation process and provides detail about the Government's consultation strategy. This section also provides a summary of key feedback from consultations, including written submissions.

5.1. Consultation Process – overview

Consultation paper engagement

On 6 August 2020, the Minister for Home Affairs announced a proposal to introduce regulatory reforms to protect critical infrastructure and *systems of national significance* as a key measure of the Cyber Security Strategy 2020. On 12 August 2020, the Minister for Home Affairs published the Protecting Critical Infrastructure and *Systems of national significance* Consultation Paper.

The Consultation Paper outlined a framework of regulatory (Positive Security Obligations, Enhanced Cyber Security Obligations and Government Assistance) and non-regulatory (Enhanced Government-Industry Partnership) proposals to protect Australia's critical infrastructure from all hazards, including dynamic cascading threats enabled by cyber attacks. It sought the views of governments, industry and

the community to shape the detail of the legislative reforms and Government's approach to implementing them on a sectoral basis.

The Department received 194 public and confidential (not released on the Department's website) submissions in response to the Consultation Paper, including submissions from all states and territories, as at the close of the submission period on 16 September 2020.

Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

On 9 November 2020, the Department released the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020, accompanied by an Explanatory Document for public consultation. Consultation closed on 27 November 2020 with Home Affairs speaking to over 1,000 individuals on the Exposure Draft Bill, with 117 formal submissions being made.

Home Affairs undertook an accessible and transparent consultation process, structured to target key stakeholders for bilateral meetings, including businesses, peak bodies and state and territory governments that could be impacted by the proposed regulations.

This approach was informed by the first round of public consultation on the Protecting Critical infrastructure and Systems of National Significance Consultation Paper and through extensive consultation with counterparts across the Australian Government, state and territory governments and industry.

Feedback received on the Exposure Draft Bill remained consistent with that received on the Consultation Paper. Consultation continued to reveal broad in-principle support for the uplift to the security and resilience of critical infrastructure and need to enhance Government's security-focused relationship with industry. Industry remains concerned about the Bill's regulatory impost, its possible duplication with existing frameworks, timeframes for implementation, and extent of the Government's intervention powers. Stakeholders have expressed gratitude for Home Affairs' genuine willingness to engage with entities on the Consultation Paper and Exposure Draft Bill.

Sector-specific surveys

Sector-specific surveys were provided to entities operating within the 11 *critical infrastructure sector*s specified in the Consultation Paper. Survey questions were designed to better understand industry views of the proposed reforms, as well as develop a clear understanding of each sector and its key cross-sector interdependencies.

The survey focused primarily on defining:

- **Relevant industry sectors**: Banking and Finance; Communications; Data and the Cloud; Defence Industry; Education and Research; Energy; Food and Grocery; Health; Space; Transport; and Water;
- **Critical functions**: relevant industry sector outputs that directly contribute to Australia's social and economic stability, defence and national security;
- **Components**: physical facilities, supply chains, information technologies or communications networks required to deliver a critical function; and
- **Operational requirements**: the systems and/or services an organisation relies upon to ensure its capabilities, technologies, and performance measures effectively deliver Components or Critical Functions (e.g. fuel supply, SCADA software updates).

Survey results have supported the Department in identifying areas of potential duplication and overlap, to avoid unnecessary or disproportionate regulatory burden within *critical infrastructure sector*s offsetting potential regulatory costs that may be incurred by industry. Information received

will continue to be used to feed into the Department's mapping and identification of Australia's *systems of national significance*.

Virtual Consultation
Town Halls

The second element of consultation in August involved six virtual town halls that were open to all members of the public to comment on the Consultation Paper. Additional town halls were held with the Business Council of Australia and the Australian Banking Association and their members. More than 620 representatives from business, civil society and state and territory governments attended these town halls, as well as 5 attendees from overseas.

Another four town halls for the Exposure Draft Bill were held in November 2020 and were open to all member of the public to comment on the Exposure Document and draft Legislation. Approximately 500 people registered for the town halls. An additional town hall was held with members of BSA (The Software Alliance) with over 100 attendees.

Sector-specific workshops

Engagement on the Consultation Paper involved 990 participants in 22 sector-specific workshops across 11 sectors (two workshops per sector). During these two-hour (on average) workshops, participants were encouraged to offer opinions and advice relating to the proposed reforms, and its application to their sector.

During the workshops, the Department worked through each sector to determine which assets should fall within the purview of the legislative reforms. The Department also sought industry's views during the workshops on existing regulatory frameworks and the costs associated with compliance.

Other engagements

For the Consultation Paper engagement, the workshops were complemented by over 30 bilateral discussions (over 400 individuals) with industry (including peak bodies) and state and territory governments to consider specific issues impacting entities and provide further input on the design of the framework.

For consultation on the Exposure Draft Bill, virtual town halls were complemented by bilateral discussions (over 400 individuals) with industry (including peak bodies) and state and territory governments to consider sector-specific issues and seek further input on the design of the framework.

These included meetings with, among others, the Business Council of Australia, Council of Financial Regulations, Australian Banking Association, Critical Infrastructure Advisory Committee, Amazon Web Services and Council of Financial Regulators Cyber Working Group.

Cyber Security Strategy 2020 engagements

Over 1,200 individuals have been engaged through the Department's public engagement efforts to message key elements of the Cyber Security Strategy 2020. This has prominently featured the Protecting Critical Infrastructure and *Systems of national significance* package.

Direct engagement with states and territories

The Department has taken an active approach to engaging with state and territory governments on these reforms. Prior to the 12 August launch, the Department arranged a round table with senior level officers from all state and territory First Ministers Offices through the National Coordination

Mechanism, outlining the objectives of the proposed reforms and intention to not duplicate or replace existing arrangements in those jurisdictions. States and territories expressed in-principle support for the reforms during this meeting.

These points were reiterated in a letter sent by the Minister for Home Affairs to all First Ministers immediately prior to the launch, which emphasised the need for officials to work in partnership to identify Australia's most critical entities and design the detail that sits underneath the features of the new framework, to ensure, wherever possible, that the reforms complement and leverage existing security regulations and initiatives within jurisdictions.

Following the launch of the reforms, the Department convened a further meeting with state and territory First Ministers' departments and relevant state and territory agencies. This meeting provided further opportunity for state and territory governments to learn more about the reforms and discuss opportunities to align and integrate with existing regulatory arrangements. These round table discussions have been complemented by a number of bilateral discussions with state and territory agencies on specific aspects of the reforms and the active involvement of states and territories in the sector specific workshops and town halls.
During consultation on the Draft Bill, Home Affairs met regularly with state and territory First Ministers' departments, briefed the National Cyber Security Committee and engaged on a bilateral basis with interested state and territory agencies. Home Affairs will continue to engage with states and territories, to ensure the views of jurisdictions are considered throughout the reforms' sectoral co-design and implementation phases.

5.2. What the Department heard and how has Government responded?

Key findings

Virtual consultations and submissions in response to the Consultation Paper and the Exposure Draft of the Bill revealed broad in-principle support for the introduction of the reforms, with certain sectors strongly supporting their inclusion within the proposed coverage of the framework, given their level of criticality and currently limited regulatory environment.

Industry concerns primarily centred on the sectoral implementation of the reforms. These included:

- The need for true co-design of sector-specific requirements and recognition that voluntary partnerships remain the first preference for resolving incidents.
- Reduce regulatory duplication by using existing frameworks where appropriate.
- Lack of clarity around the definition of critical infrastructure sectors and assets and *systems of national significance*.
- Unclear and possibly high regulatory impost, as well as possible duplication with existing regulatory frameworks (particularly in sectors with existing, mature security frameworks).
- Timeframes for implementing these reforms.
- Lack of consultation on an exposure draft of proposed legislative amendments to SoCI.
- Extent of the proposed Government Assistance powers.
- Costs associated with the reforms.

At the core of these reforms will be an enhanced Government-industry relationship, focused on partnerships with industry and outcomes-based compliance mechanisms. In response to industry concerns, the reforms will feature clear coverage, as outlined in primary legislation, with appropriate implementation and co-design timeframes that leverage existing regulations to balance regulatory impost with security outcomes. Government Assistance measures will also be limited by robust oversight mechanisms and in order to provide further opportunity to key stakeholders to refine the legislative reforms, the Department also released and consult on an exposure draft of the Bill with an accompanied explanatory document.

Supporting the need for reform

Industry, states and territories have expressed broad support for, and understanding of, Governments decision to introduce an enhanced critical infrastructure security regulatory regime. The Department heard that Australia's current critical infrastructure regulatory arrangements need strengthening to build the nation's security posture.

The Department worked closely with stakeholders across sectors to determine appropriate thresholds for the reforms' obligations. Submissions showed support for the 11 sectors identified by the Government. A number of organisations self-identified as *critical infrastructure assets* to be covered by the reforms.

Some stakeholders proposed alternative approaches to building critical infrastructure security and resilience. These included, for example, a vulnerability disclosure scheme; national critical services overlay network; use of environmental surveillance network instrumentation to show changes to risk leading indicators in near real time. However, these suggestions were piecemeal and ultimately aligned with Government's security objectives.

Reduce regulatory duplication with existing regulatory frameworks

Industry and governments remain concerned with the Bill's regulatory burden, and interactions between the measures proposed and existing regulatory frameworks. Some stakeholders have called for obligations across sectors to be harmonised or Government leverage domestic or international standards, to achieve a consistent security uplift.

Home Affairs notes that the Bill embeds the need to reduce regulatory duplication throughout the regime by, for example, requiring the Minister to consult with industry on the introduction of Rules (s 30AL), implement the Positive Security Obligation on a sectoral-basis by 'switching on' obligations (ss 30AB, 30BB, 18A), and exercise Government Assistance measures only where other regulatory measures cannot be used (s 35AB). Home Affairs shares industry's view that the reforms should reduce regulatory duplication and will continue to engage with entities to identify and mitigate areas of duplication.

On Coverage

Some stakeholders called for clarity over the coverage of the reforms. Others stated a preference for greater flexibility, by setting thresholds in delegated legislation. The Department has engaged with participants from each sector to help workshop and design the coverage of each of the reforms' measures. This also included workshopping the definition of *critical infrastructure sector* and *critical infrastructure assets* with Commonwealth counterparts, industry and peak bodies to ensure that only those assets that should be captured by the reforms are captured. For example:

- The Department has worked with industry and Commonwealth counterparts to refine the 'critical broadcasting asset' definition. Notably, amendments were made to exclude retransmission assets unless they are prescribed by the rules. This change takes into account concerns that the inclusion of all retransmission assets did not serve the policy intent and would place an unreasonable regulatory burden on their owners and operators.
- The financial service and markets sector sectoral definition, and the sector's critical infrastructure asset definitions, were shaped by input from Commonwealth partners and existing financial regulators. For example, the Department incorporated input on what should be included in the financial services and markets sector definition, and which assets within the sector should be captured as critical infrastructure assets. This also included a shift in terms of

the criticality for financial services and markets sector critical infrastructure assets to be focused on entities rather than their assets.

- The Department worked with industry and Commonwealth counterparts to refine the definition of "critical liquid fuels assets". Originally the definition proposed a legislated volume threshold to capture liquid fuel storage takes, however consultation with industry indicated that such a threshold may be difficult to enforce and may cause confusion over who is and is not regulated. Instead, it has been proposed that a broad definition of a liquid fuel storage terminal be included in the legislation with the Rules to be developed with industry to ensure that the appropriate assets are covered, also allowing flexibility as the industry changes.
- The threshold for a "critical water asset" has not been altered from the original definition currently with SoCI. The idea of using a principles based test for what is or is not a critical water asset was suggested by industry, however further discussion with industry and the Commonwealth determined that such a method would not provide industry with enough certainty in the legislation around who is and who isn't covered. It was ultimately agreed with industry that retaining the current thresholds was the best course of action.

Leveraging existing regimes and reducing regulatory impost

Stakeholders expressed concern over the regulatory impost of the reforms. Stakeholders emphasised the need to reduce this burden by co-designing the Positive Security Obligations with industry and leveraging existing frameworks. It was noted that smaller critical infrastructure providers would be required to do comparably more to build security and resilience. Some members of industry suggested the Positive Security Obligations remain principles-based to avoid over-regulation. Other stakeholders advocated for a clear set of obligations for industry operators to provide regulatory clarity for operators.

Stakeholders across sectors clearly articulated the need to reduce duplication with existing frameworks. States and territories called for alignment with existing jurisdictional requirements. A number of stakeholders pointed to existing international standards and examples of best practice. Stakeholders agreed that Government will need to work with operators to develop and implement the Positive Security Obligations in way that reduces its impost. Industry recommended that Government and operators work together to better understand and reduce the economic impacts of the reforms, as critical infrastructure assets would not presently able to provide cost estimates.

The Department is committed to reducing duplication and unnecessary regulatory impost by identifying potential offsets through the co-design of the risk management program. The Department will work in tandem with industry and existing regulators to develop and implement the Positive Security Obligations. Key to this process will be the identification of sector regulators and existing regulatory standards, guidance or international exemplars that:

- meet the Positive Security Obligation's high-level security outcomes; and
- meet the needs of the sector's operators and regulator.

During this process, the Department will work with entities to conduct economic modelling on a sectoral basis to draw out key risks and impacts, and build this information in to the Positive Security Obligation's co-design.

Enhanced Cyber Security Obligations

Through consultation, industry has also clearly articulated that the Enhanced Cyber Security Obligations must be proportionate to entities' cyber risks and consequences. To meet this requirement, only a limited subset of entities are expected to be subject to these obligations. Coverage will be informed by work being undertaken by the CIC to map critical infrastructure

interdependencies, identify the nation's most critical entities, and support the Minister's designation using a methodology tested with industry and government. The methodology considers sectors' critical functions, the reliance of others on those functions, and their operational features of each sector. This enables the identification of entities that would represent a systemic threat if compromised, due to the significant number of critical functions across sectors directly or indirectly impacted.

Government Assistance

Industry consultation on the Government Assistance measure has revealed cautious support. Industry reiterated the need for appropriate thresholds and oversight, and recognition that voluntary partnerships remain the Government's first preference for resolving incidents. In response to this feedback, it is proposed that the Secretary of Home Affairs, on advice from relevant organisations, will have the power to seek an authorisation from the Minister for Home Affairs to take steps to prevent, mitigate or restore functionality of an asset following a nationally significant cyber incident, if an entity is unable or unwilling to do so. The proposed option will cover any asset within a *critical infrastructure sector*, to ensure the Government can effectively intervene if there were a nationally significant cyber incident impacting critical infrastructure. This broader scope will ensure the Government can take necessary steps to manage significant risks at appropriate points in the supply chain of *critical infrastructure asset*s.

Co-design and implementation are key

Industry, states and territories expressed strong concern over the short timeframe allocated for consultation on the enhanced legislative framework. Entities are keen to work closely once the co-design process is initiated. In light of the short consultation timeframes, a number of stakeholders across industry, states and territories additionally called for release of an Exposure Draft of the Bill.

The Department has engaged in targeted engagement with sectors to consider the details of the legislative framework, with sectoral co-design of requirements giving effect to the Positive Security Obligations to occur in late-2020 to mid-2021. Prior to introduction of the Bill to Parliament, the Department released an Exposure Draft of the legislative reforms to seeking further feedback from operators on thresholds and obligations outlined in the draft Bill.

Building a Government-Industry partnership through ongoing engagement

Stakeholders recognised that key to the required uplift of security and resilience in Australia's critical infrastructure, is an enhanced relationship between operators and governments. The Department heard that the Government's non-regulatory engagement with operators needs to be strengthened. Stakeholders advised that the value of the TISN has diminished and that its reinvigoration would require genuine and valuable information exchange, and guidance from Government. Industry noted that expansion of the TISN, in line with the reforms' coverage, will bring additional insights and information sharing to the networks.

A number of submissions called for monetary support from Government to assist them uplift their security and comply with legislative obligations.

The Department is committed to building its voluntary engagement mechanisms, including through the TISN. The Department is exploring a number of measures to improve Government's operator engagement and build a collective understanding of risk within and across sectors, including by: co-designing best practice guidance; providing all hazard threat assessments; and, introducing a two-way industry-government secondment program. This support will assist entities meet their legislated obligations, as well as building the security and resilience of non-regulated entities. Through the

Cyber Security Strategy 2020, the Department is also building its cyber security industry outreach capability by establishing a permanent presence within the Joint Cyber Security Centres.

Importantly, engagement with industry does not end here. Co-design of the sector-specific approaches is expected to continue into early 2021 to both meet the needs and appropriately lift the capabilities of regulated entities. This includes working closely with entities and regulators to prepare sector-specific guidance and provide clear understanding of the requirements of the Risk Management Program under the Positive Security Obligations, and who will be required to report to the Register of Critical Infrastructure and engage in Mandatory Cyber Reporting. This will be influenced heavily by existing regulations experienced currently by each sector. This will also enable the Government to build on its current partnership with industry to develop a stronger and more collaborative approach to engagement, communication and information sharing.

The role of states and territories

In round tables and in bilateral meetings, state and territory agencies have highlighted the importance of aligning these reforms with existing arrangements in their jurisdictions and working in partnership with the Commonwealth to design and implement these reforms. States and territories have the opportunity to be involved in the co-design of the sector specific standards, information sharing arrangements and the Government Assistance measures. The Tasmanian Government told the Department, "any powers developed that give the Australian Government the ability to declare a sector specific emergency should only be done in consultation with jurisdictions, and then only by the relevant portfolio/sector minister". Industry stakeholders also identified that collaboration with states and territories could assist in building security outcomes. Industry advised that, for example, state and local government agreement could be sought to enhance physical security by security perimeters around critical assets.

The Department will continue to work with states and territories throughout the implementation of these reforms to build information sharing capability across jurisdictions and leverage existing security relationships. The Department will continue to work with Commonwealth agencies and states and territories to uplift the security and resilience of Australia's Government and Democracy.

5.3. Risk management program – co-design process to address stakeholder concerns

Partnerships with industry sit at the foundation of these reforms. As such, consultation will not end with the introduction of the enhanced legislative framework. 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, ensuring costs are offset to minimise regulatory 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 addresses any concerns they may have, balanced against Government's policy objectives to uplift critical infrastructure resilience and security against all hazards.

The co-design period will commence in early 2021 and will be phased on a sector by sector basis over a period of 18 months. During co-design the Department, Commonwealth and state and territory agencies, sector regulators, and key industry stakeholders will work closely together to develop the sector-specific requirements that underpin the risk management program. It will be important to take this time to ensure these requirements clearly outline expectations, and what would be considered a reasonable and proportionate response to meeting this element of the Positive Security Obligation.

Undertaking a co-design process will ensure the specific requirements:

- 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.

To offset costs to industry, wherever possible, the Positive Security Obligation provides an on-switch mechanism to activate the elements of the obligations including the risk management program. 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 obligations will remain dormant, with those existing obligations continuing to apply without duplication.

- 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 – ensuring no duplication of regulatory burden for Australia's defence industry.

It is clear the risk management program will have a regulatory impact on industry, while recognising the concurrent benefits to the economy, national security and sovereignty of Australia. The depth and breadth of this economic impact will vary based on the existing maturity within sectors and the scope of the sector-specific rules. To ensure there is a collective understanding across Government and industry of the impact of these reforms and addresses any concerns, Home Affairs will procure economic modelling experts to assess the anticipated regulatory impact of uplifting the security and resilience of Australia's critical infrastructure. This will allow robust economic modelling across the critical infrastructure sectors as part of the development of the sector specific rules and guidelines to assist in the interpretation of the rules. The economic modelling will form a key aspect of engagement with industry and government during the co-design process and will focus on a number of key elements:

- Provide a breakdown of the administrative compliance costs to industry in meeting the risk management program.
- Provide a breakdown of other substantive costs to industry as a result of the risk management program.
- Develop scenarios to assess the administrative and substantive compliance costs. These scenarios would consider the directions and actions likely to be issued in different situations and the impact of these on owners and operators.
- Outline costs to industry in terms of staffing, skill requirements and time commitments.
- The potential returns on additional investment required to meet the risk management program.
- The savings from a reduced frequency of security incidents, and the costs to owners and operators should no action be taken.

6. WHAT IS THE BEST OPTION FROM THOSE YOU HAVE CONSIDERED?

This Regulation Impact Statement recommends that the Government pursue Option Two through targeted regulatory action involving a Positive Security Obligations, an Enhanced Cyber Security Obligation, Government Assistance and an expanded Ministerial Direction power which will all be underpinned by an enhanced Government-industry partnership through the TISN.

As outlined below Option Two most effectively responds to the policy problem outlined in section 1. Critical infrastructure is increasingly interconnected and interdependent and this interconnectivity has created an evolving and increasing set of threats. Without enforceable safeguards, vulnerabilities can deliberately or inadvertently cause disruption that could result in catastrophic and cascading consequences across Australia's social and economic stability, defence and national security. It is

appropriate that the Government takes regulatory action to support the business community to combat this issue.

6.1. Option Two – Legislative change, a compliance and assurance capability

This Regulation Impact Statement assesses that Option Two is likely to deliver the greatest benefit in terms of providing industry with consistent direction, assistance and guidance that will provide an uplift in security across all critical infrastructure, safeguarding Australia's social and economic stability, defence and national security.

This will support business to better address the risks to critical infrastructure and assist investors and consumers with their investing decisions and long term business plans through greater clarification and consolidation of security requirements. The benefits arising from these cost are commensurate with: the Government's objectives for reform; the nature and extent of risks to critical infrastructure; the benefits of the regulation and the creation of a level playing field for industry.

The maximum aggregated, annual costs to industry as a result of the Register of Critical Infrastructure Assets and the mandatory cyber reporting are estimated at $2.19 million annually. This cost does not include the Enhanced Cyber Security Obligations or the Ministerial Directions power as these elements of the reforms do not require ongoing industry obligations but rather are upon request. Consequently, where a request is made the ESCO and Ministerial Directions are expected to cost industry the following:

- **ECSO** (applicable only to SoNS):

Incident response plans – maximum annual compliance burden $28,091.30 for a single SoNS assuming annual requirements.
Telemetry - maximum annual compliance burden $81,250 for a single medium SoNS and $361,250 for a single large SoNS assuming annual requirements.
Vulnerability assessments - maximum annual compliance burden $46,875 for a single medium SoNS and $117,375 for a large SoNS assuming annual requirements.
Cyber Security exercises - maximum annual compliance burden $61,425 for a single SoNS assuming annual requirements.

- **Ministerial Directions** (applicable to all *critical infrastructure sector* assets):

Scenario 1 – annual compliance burden for this scenario is estimated at $4,999 on average per entity assuming the direction power will be used once every three years.
Scenario 2 - annual compliance burden for this scenario is estimated at $280,741 on average per entity assuming the direction power will be used once every three years.
Scenario 3 - annual compliance burden for this scenario is estimated at $279,541 on average per entity assuming the direction power will be used once every three years.

However, it is considered that these costs are outweighed by the benefits provided by these reforms through addressing the key aspects of the policy challenge outlined within section 1.

6.1.1. Increase the resilience of Australia's critical infrastructure from all hazards

The reforms will ensure entities take an all-hazards approach when identifying risks that may affect the availability, integrity, reliability and confidentiality of their assets. This will require consideration of both natural and human induced hazards which pose a material risk. 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.

Whilst Option Two will have the highest regulatory impost, these costs must be considered within the broader context of the savings that can be created by increasing critical infrastructure resilience and reducing the likelihood and severity of incidents. It is estimated that cyber security breaches cost the Australian economy approximately $29 billion per year[17] with natural disasters costing more than $13 billion per year and expected to rise to $39 billion per year by 2050.[18] Even a modest saving as a result of Government and industry investment in these reforms will represent a significant cost saving to industry and Australian consumers.

6.1.2. Protection against physical, cyber, supply chain and personnel domains

It is intended that the risk management programs under the PSO will require entities to take into account material risks, whether natural or human induced hazards, encouraging a holistic risk management approach in the safeguarding of critical infrastructure. At a minimum, it is proposed that sector-specific rules, to be developed with industry, will require responsible entities to consider and address risks within these four domains. This will enable entities to better prepare for and respond to significant security incidents regardless of source or vector.

6.1.3. Increasing threats, connectivity and complexity of critical infrastructure

The reforms respond to clear concerns raised during public consultations for the Australian Cyber Security Strategy, and consultation held in response to the proposed reforms, around the risks posed by the connectivity and complexity of critical infrastructure. Specifically, stakeholders noted the importance of the Government uplifting security and resilience in critical infrastructure especially in the face of increasing interconnectivity.

In particular, concentrating critical infrastructure resilience within the Department of Home Affairs through the proposed reforms enables a coordinated, national approach toward the management of critical infrastructure. Currently, the management of critical infrastructure sectors and assets are categorised by sector, or according to state and territory jurisdictions. The envisioned reforms enable the Department of Home Affairs to build awareness and management of issues that cut across critical infrastructure sectors, while recognising relevant regulations that exist in particular sectors or state and territory jurisdictions.

6.1.4. Existing legislative arrangements are insufficient for the current threat environment

If a significant cyber incident on critical infrastructure happened today, there is a risk that the Government may not have the mechanisms to act decisively to support an entity to stop or prevent an attack, nor does industry have obligations to report significant cyber incidents or apply minimum cyber security standards. Key gaps in current legislative arrangements relate to Government lacking the ability to assist assets during exceptional cyber security incidents.

The proposed reforms address these issues:

- the Positive Security Obligations which will set and enforce baseline protections for critical infrastructure assets, implement sector specific standards and strengthen sectoral regulatory oversight;

[17] Microsoft and Frost and Sullivan, 2018, Understanding the Cybersecurity Threat landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World.
[18] Deloitte Access Economics, 2017, Building resilience to natural disasters in our states and territories, file://din.bcz.gov.au/users/CBR01/JT97ZF/home/Downloads/deloitte-au-economics-building-resilience-natural%20disasters-states-territories-161117.pdf.

- the Enhanced Cyber Security Obligation which will provide a framework for 'incident response plans' setting out response arrangements, build a near real-time threat picture and further strengthen the cyber resilience of *systems of national significance*; and
- the Government Assistance will ensure the Government has the ability to respond in an effective and timely manner to nationally significant cyber security attacks in exceptional circumstances.

6.1.5. The Government currently has limited visibility and power to act

Without compulsory requirements around the management of critical infrastructure, the Government will have limited abilities to:

- Create an accurate picture of emerging threats (whether cyber or otherwise), and address potential inconsistencies across sectoral approaches to critical infrastructure
- Monitor and enforce compliance around the management of security for critical infrastructure, and
- Provide assistance to support a responsible entity to stop or prevent a cyber-attack.

This gap is addressed through the introduction of the Positive Security Obligation, Enhanced Cyber Security Obligations and Government Assistance measures collectively. These measures will provide both Government and Industry with the necessary tools to identify, deter and mitigate potential security incidents as well as appropriately respond to security incidents that do occur.

6.1.6. Regulation is wanted and needed to drive a wholesale uplift in security and resilience

Multiple phases of consultation have shown broad industry support for the Government to proceed with the development and implementation of the regulations and an enhanced collaboration between the Government and industry.

> *"Although industry should lead, in the sense that it accepts principal responsibility for its own security, the essential role of Government is to create the environment and the opportunities for consultation, coordination and collaboration in and between all critical infrastructure sectors and* beyond*, leading to cultural change and to wide acceptance that security, in all its forms, is a plus for business and not a cost to be endured."* – CyberOps.[19]

Without a clear and consistent approach established in regulation it can also be difficult for businesses to justify expenditure on uplifting all hazards security practices, or even to confidently identify which material risks should be prioritised. This will be addressed by the reforms, which establish over-arching standards.

6.3 Alternate options

Option 3: Maintain the status quo

This RIS canvasses the impact of maintaining the status quo (section 4). Failing to actively encourage a sustained uplift in critical infrastructure resilience will mean the threats to critical infrastructure will continue, if not intensify. The interconnected nature of our critical infrastructure means that compromise in one essential function can have a domino effect that degrades or disrupts others.

Recent events, particularly COVID-19, have demonstrated how threats can have flow on effects across multiple sectors:

[19] CyberOps, Submission provided 24 September 2020, page 12. https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/Submission-009-CyberOps.PDF.

- Over the last two years, we have seen several cyber-attacks in Australia that have targeted the Federal Parliamentary Network, airports and universities.
- 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.
- Key supply chain businesses transporting groceries and medical supplies have also been targeted.

As discussed within section 3, an operability disruption has been modelled for each critical infrastructure sector to provide an estimate of the cost to the Australian economy. While uncertainty around the likelihood and severity of all hazards makes it almost impossible to know the exact costs of an operability disruption, it is estimated that a 10 per cent operability disruption over one week will cost between $0.06 billion to $3.0 billion depending on the critical infrastructure sector.

Further, extensive consultations with Commonwealth, State and Territory counterparts and industry has highlighted support for reforms. Specifically, industry has recognised the increasing vulnerability of critical infrastructure and the need to implement meaningful safeguards. During consultation UniSys noted that "*[t]he opportunity cost of not being cyber resilient must also be considered. For example, in the area of cyber risk management it is important that organisations are able to communicate cyber risk to Boards and Executives. This is one of the key reasons why businesses underinvest in cyber security and addressing this will ultimately lead to better cyber resilience for businesses."*[20]

Option 3: Voluntary obligations

Option three contemplates no legislative change, encouraging critical infrastructure resilience through voluntary engagement through the Trusted Information Sharing Network and publishing additional guidance alongside the updated Critical Infrastructure Resilience Strategy.

Industry consultations has highlighted the value of creating uniform, consistent, mandatory standards around the management of critical infrastructure assets. Risk professionals have argued that without clear mandatory standards, it has been difficult to drive organisational changes that uplift security practices. Without clear risk management standards and the ability to monitor and enforce compliance, Government cannot be adequately assured that appropriate risk mitigation of critical infrastructure is in place.

While voluntary obligations will go some way toward addressing the policy problem – for instance encouraging a holistic consideration of material risks that may affect critical infrastructure – implementing the mandatory requirements in Option Two while enlivening mechanisms to enhance partnerships with private industry will provide a greater degree of certainty for industry and assurance to the Government that national security risks to critical infrastructure are being managed.

7. HOW WILL YOU IMPLEMENT AND EVALUATE YOUR CHOSEN OPTION?

This section sets out how the Government proposes to implement and evaluate the proposed regulatory changes.

7.1. Implementation Plan

The Government aims to implement the proposed measures in a way that ensures:

[20] Unisys, Submission provided 24 September 2020, page 4, https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/Submission-011-Unisys.PDF.

- Relevant entities understand and comply with their obligations,
- Relevant entities, critical infrastructure owners and operators engage with the Government to understand risks and collaborate to drive effective baseline security standards,
- Robust economic modelling is undertaken ahead of sector specific rules being made,
- Appropriate powers to respond in the event of cyber security incident,
- Relevant entities receive appropriate and consistent direction, assistance and guidance from the Government to comply with the obligations and support an uplift in security posture, and
- National security risks in entities' operations and supply chains are identified, assessed and mitigated.

A timetable for implementation and key tasks is set out below.

Activity	**Estimated date**
Mapping of *critical infrastructure sector*s, identification of *systems of national significance*.	May 2020 – ongoing
Identification of regulators, regulator uplift.	May 2020 – February 2021
Cost benefit analysis	July 2020 – ongoing
Drafting of legislation	August 2020 – November 2020
Introduction of legislation to Parliament, referral to Parliamentary Joint Committee for Intelligence and Security.	December 2020
Legislation considered.	Autumn sitting period 2021
Education and engagement program.	January – July 2021
Co-design of sector specific standards with industry.	January 2021 - ongoing
Economic modelling of sector specific obligations and subsequent RIS/s.	January 2021 - ongoing
Preparation of guidance for industry on compliance with new obligations.	January 2021 - ongoing
Preparation for enforcement of legislated obligations.	Ongoing as Rules are established
Government Assistance and Enhanced Cyber Security Obligations commence. Positive Security Obligations commences. Six month grace period before enforcement of obligations.	1 July 2021
Enforcement of PSO commences	1 January 2022

Post-Implementation Review	2026

7.2. Legislation

To meet the Government's objectives, the Government will develop and introduce into Parliament amendments to SoCI, and associated regimes where necessary, to establish the legal framework for the enhanced critical infrastructure security framework. To assist in the development of the legislative amendments, and support their implementation by industry, the Department will undertake a range of preparatory activities.

The Department has worked with key sectors to identify which entities should fall under the purview of amended SoCI and those that are to be declared as *systems of national significance*.

The Government aims to have the amendments developed and introduced to Parliament by the end of 2020, The Government Assistance powers will commence upon Proclamation. The Enhanced Cyber Security Obligations will also commence upon Proclamation. However, these obligations would not be imposed on any entity until the Minister has designated an asset as a *system of national significance*. The Positive Security Obligations will commence upon Proclamation. However, these obligations will not be applied to critical infrastructure assets until the sector-specific co-design has been completed and the sector-specific rules have been made. There will be a six month 'grace period' following the introduction of the sector specific rules.

7.3. Establishing regulatory functions

To implement the proposed divested model of security obligations and compliance, the Department will engage with appropriate regulators. Alongside the development, introduction and passage of legislation, the Department has worked with Commonwealth agencies and state and territory governments to identify appropriate regulatory bodies to enforce the proposed security obligations. Where no regulatory body exists or is willing to undertake this role, the Department will be the regulator.

The Department and identified regulators will collaborate on sector specific guidance for entities to assist them reach compliance with the new security obligations. Guidance may include case studies, clear definitions, frequently asked questions, threat information, risk advice, tips on best-practice and additional information about the Government's expectations. The Government will draft this guidance in consultation with industry and sectors experts and bodies. This guidance will be made available as soon as practicable after legislation is passed.

Critical Infrastructure Centre (CIC)

To undertake the above activities, the Department will expand the CIC to engage a significant number of staff and contractors with key subject matter and technical expertise, as well as dedicated staff to undertake industry engagement. The Centre will also draw on the expertise of secondees from other Australian Government agencies to ensure that the proposed amendments are developed and implemented through collaboration across the Government. The Australian Signals Directorate's expertise will ensure alignment with the CESAR capability and help entities to meet their Enhanced Cyber Security Obligations.

In meeting their Enhanced Cyber Security Obligations, entities will provide information to the Australian Cyber Security Centre. The Australian Cyber Security Centre will analyse information provided, determine the need for preparatory assessments and activities and report back to the entity.

Where appropriate, the Australian Cyber Security Centre will share near-real time threat information. Entities would be expected to take steps to minimise potential cyber threats as appropriate.

The Australian Cyber Security Centre and CIC will work closely together to determine if Government Assistance is required to prevent, disrupt or respond to an incident identified by the Government or reported by an entity.

The Department will also regulate certain sector's Positive Security Obligations where no alternative regulator has been identified. The costs of this responsibility will be detailed in future RIS(s) and be available in Budget papers.

Reporting

The Department will report on the implementation of the proposed measures in its annual report to Parliament under section 60 of the Act.

7.4. Challenges / risks to implementation

There are several key risks to the successful implementation of the proposed regulatory changes and enhanced Government-industry engagement: lack of awareness of the new obligations, lack of proper implementation and engagement with regulations by industry, and lack of government capability to enforce compliance.

Awareness

As part of the development of the reforms and proposed legislative changes, the Department has and is continuing to lead detailed stakeholder consultation with critical infrastructure providers across Australia, state and territory governments, and other relevant entities on the proposed legislative reforms. This includes bilateral meetings, industry roundtables and open forums. As a result, it is unlikely any affected entities will be surprised by the proposed legislation or the extent of obligations.

Uptake

For the proposed obligations to be successfully implemented, the Government must ensure that key stakeholders (including critical infrastructure owners and operators, states and territories and international investors) recognise the net benefit associated with this proposal. Strong stakeholder support and engagement is important to maximising implementation of the reforms by industry, and their success in producing real risk outcomes and security uplift. Industry cooperation with, and the effectiveness of, the Government's emergency step-in powers will also rely on positive and constructive relationships between the Government and industry.

Consultations over the last few years have shown broad industry support for the Government to proceed with the development and implementation of the regulations and enhanced Government-industry engagement. This includes strong support from large businesses that would be covered by the proposed regulation. The Department has engaged widely to ensure industry support for the regulatory changes proposed, and will engage in extensive industry consultation and co-design of security standards, as well as a roadshow (physical or virtual) following passage of legislation to ensure industry buy-in and to provide guidance to assist entities to meet their new obligations.

The Department has, and will continue to, work closely across the Government and with industry stakeholders to ensure any new regulatory obligations are not duplicative or overly burdensome for stakeholders.

Government capability

To address this risk, the Department will undertake a significant hiring and training program to ensure officials engaging with industry are knowledgeable security professionals, highly skilled at identifying vulnerabilities in specific assets and are able to recommend effective mitigations to manage those risks. Enhancing capability at the Government level will also be undertaken to understand and assess compliance with security obligations. The funding in this proposal will support the recruitment of staff with specific expertise including compliance, assurance and data analysis skills as well as contracting private sector technical and cyber security expertise. Staff will be trained to become security experts, highly skilled at identifying vulnerabilities in specific assets and recommending effective mitigations to manage those risks.

The staffing levels needed to effectively implement the proposed changes will be provided to the Government for consideration as part of funding proposals for later years. The level of staffing will depend heavily on the outcomes of the co-design with industry early next year.

7.5. Monitoring and evaluation

The effectiveness of the reforms will be assessed on an ongoing basis, including the annual report to Parliament, Senate Estimates processes and feedback from stakeholders including, other Government regulators business and industry. Mechanisms for review include:

- Reporting: Section 60 of SoCI currently requires an annual report to Parliament on directions made, regulatory action undertaken, information sought and assets declared. These will be expanded to require reporting on the exercise of the proposed new powers under option 2.
- Assurance: there will be a whole of government compliance and assurance capability designed to enhance compliance with existing legislation and to engage with industry on risk. Through this, the Department will routinely evaluate performance of the reforms during and after implementation. Evidence of adoption of standards and practices by industry will be available to the Department on an ongoing basis as it manages the reporting, information gathering and enforcement of the Positive Security Obligations component of the reforms. Regulators will be responsible for providing assurance to the Government that obligations are being met.
- Engagement: Informal review of implementation and policy effectiveness will be an ongoing part of the Department's engagement with industry through the revitalised TISN program. Industry uptake and engagement with the voluntary assistance program will also provide a key source of data that will inform development of the reforms.
- In the event of a significant cyber security incident involving government intervention, a post-action review will be undertaken to assess the effectiveness of arrangements and make recommendations for future preparedness.

7.6. What will success look like?

If the proposed reforms are successful, the Government, industry and the Australian public will have greater confidence in the resilience of our critical infrastructure providers through a clear uplift in all hazards risk management. The Government and industry will share near real-time threat information to mitigate risks, and have the authorities and capabilities to respond to a significant incident. Importantly for our bilateral relationships, Australia will rely less on foreign investment review frameworks to mitigate risks and support the rules-based order. Economic openness and investment attraction will be maintained and not impede improved risk management.

Attachment A

Critical Infrastructure Asset	Thresholds
Critical telecommunications asset	(1) critical telecommunications asset means: a) a telecommunications network that is: a. owned or operated by a carrier; and b. used to supply a carriage service; or b) a telecommunications network, or any other asset, that is: a. owned or operated by a carriage service provider; and b. used in connection with the supply of a carriage service.
Critical broadcasting transmission asset	(1) One or more broadcasting transmission assets are a critical broadcasting asset if: a) the broadcasting transmission assets are: a. owned or operated by the same entity; and b. located on a site, that, in accordance with subsection (2), is a critical transmission site; or b) the broadcasting transmission assets are: a. owned or operated by the same entity; and b. located on at least 50 different sites; c. not broadcasting re-transmission assets; or c) the broadcasting transmission assets are owned or operated by an entity, that, in accordance with subsection (3), is critical to the transmission of a broadcasting service.
Critical domain name system	An asset that: a) is managed by entity, that, in accordance with subsection (2), is critical to the administration of an Australian domain name system; and b) is used in connection with the administration of an Australian domain name system.
Critical data storage or processing asset	An asset is a ***critical data storage or processing asset*** if: a) it is owned or operated by an entity that is a data storage or processing provider; and b) it is used wholly or primarily to provide a data storage or processing service that is provided by the entity on a commercial basis to an end-user that is: (i) the Commonwealth; or (ii) a body corporate established by a law of the Commonwealth; or (iii) a State; or (iv) a body corporate established by a law of a State; or (v) a Territory; or (vi) a body corporate established by a law of a Territory; and c) the entity knows that the asset is used as described in paragraph (b).
Critical Defence industry asset	(1) critical defence industry asset means an asset that: (a) is being, or will be, supplied by an entity to the Defence Department, or the Australian Defence Force, under a contract; and (b) consists of, or enables, a critical defence capability.
Critical banking asset	(1) An asset is a ***critical banking asset*** if it is any of the following assets: (a) an asset that:

	(i) is owned or operated by an authorised deposit-taking institution, that, in accordance with subsection (2), is critical to the security and reliability of the financial services and markets sector; and (ii) is used in connection with the carrying on of banking business; (b) an asset that: (i) is owned or operated by a body corporate that is a related body corporate of an authorised deposit-taking institution and that, in accordance with subsection (3), is critical to the security and reliability of the financial services and markets sector; and (ii) is used in connection with the carrying on of banking business. Note: The rules may prescribe that a specified critical banking asset is not a critical infrastructure asset (see section 9). (2)For the purposes of subparagraph (1)(a)(i), the rules may prescribe: (a) specified authorised deposit-taking institutions that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for an authorised deposit-taking institution to be critical to the security and reliability of the financial services and markets sector. (3)For the purposes of subparagraph (1)(b)(i), the rules may prescribe: (a) specified bodies corporate that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for a body corporate to be critical to the security and reliability of the financial services and markets sector.
Critical superannuation asset	(1)An asset is a ***critical superannuation asset*** if: (a) it is owned or operated by a registrable superannuation entity, that, in accordance with subsection (2), is critical to the security and reliability of the financial services and markets sector; and (b) it is used in connection with the operation of a superannuation fund. Note: The rules may prescribe that a specified critical superannuation asset is not a critical infrastructure asset (see section 9). (2)For the purposes of paragraph (1)(a), the rules may prescribe: (a) specified registrable superannuation entities that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for a registrable superannuation entity to be critical to the security and reliability of the financial services and markets sector.
Critical insurance asset	(1) An asset is a critical insurance asset if it is any of the following assets: (a) an asset that: (i) is owned or operated by an entity that carries on insurance business and that, in accordance with subsection (2), is critical to the security and reliability of the financial services and markets sector; and (ii) is used in connection with the carrying on of insurance business; (b) an asset that: (i) is owned or operated by a body corporate that is a related body corporate of an entity that carries on insurance business and that, in accordance with subsection (3), is critical to the security and reliability of the financial services and markets sector; and (ii) is used in connection with the carrying on of insurance business; (c) an asset that:

	(i) is owned or operated by an entity that carries on life insurance business and that, in accordance with subsection (4), is critical to the security and reliability of the financial services and markets sector; and (ii) is used in connection with the carrying on of life insurance business; (d) an asset that: (i) is owned or operated by a body corporate that is a related body corporate of an entity that carries on life insurance business and that, in accordance with subsection (5), is critical to the security and reliability of the financial services and markets sector; and (ii) is used in connection with the carrying on of life insurance business; (e) an asset that: (i) is owned or operated by an entity that carries on health insurance business and that, in accordance with subsection (6), is critical to the security and reliability of the financial services and markets sector; and (ii) is used in connection with the carrying on of health insurance business; (f) an asset that: (i) is owned or operated by a body corporate that is a related body corporate of an entity that carries on health insurance business and that, in accordance with subsection (7), is critical to the security and reliability of the financial services and markets sector; and (ii) is used in connection with the carrying on of health insurance business. Note: The rules may prescribe that a specified critical insurance asset is not a critical infrastructure asset (see section 9). (2) For the purposes of subparagraph (1)(a)(i), the rules may prescribe: (a) specified entities that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for an entity to be critical to the security and reliability of the financial services and markets sector. (3) For the purposes of subparagraph (1)(b)(i), the rules may prescribe: (a) specified bodies corporate that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for a body corporate to be critical to the security and reliability of the financial services and markets sector. (4) For the purposes of subparagraph (1)(c)(i), the rules may prescribe: (a) specified entities that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for an entity to be critical to the security and reliability of the financial services and markets sector. (5) For the purposes of subparagraph (1)(d)(i), the rules may prescribe: (a) specified bodies corporate that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for a body corporate to be critical to the security and reliability of the financial services and markets sector. (6) For the purposes of subparagraph (1)(e)(i), the rules may prescribe: (a) specified entities that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for an entity to be critical to the security and reliability of the financial services and markets sector. (7) For the purposes of subparagraph (1)(f)(i), the rules may prescribe:

	(a) specified bodies corporate that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for a body corporate to be critical to the security and reliability of the financial services and markets sector.
Critical financial market infrastructure asset	(1)An asset is a ***critical financial market infrastructure asset*** if it is any of the following assets: (a) an asset that: (i) is owned or operated by an Australian body corporate that holds an Australian market licence; and (ii) is used in connection with the operation of a financial market, that, in accordance with subsection (2), is critical to the security and reliability of the financial services and markets sector; (b) an asset that: (i) is owned or operated by an associated entity of an Australian body corporate that holds an Australian market licence; and (ii) is used in connection with the operation of a financial market, that, in accordance with subsection (2), is critical to the security and reliability of the financial services and markets sector; (c) an asset that: (i) is owned or operated by an Australian body corporate that holds an Australian CS facility licence; and (ii) is used in connection with the operation of a clearing and settlement facility, that, in accordance with subsection (3), is critical to the security and reliability of the financial services and markets sector; (d) an asset that: (i) is owned or operated by an associated entity of an Australian body corporate that holds an Australian CS facility licence; and (ii) is used in connection with the operation of a clearing and settlement facility, that, in accordance with subsection (3), is critical to the security and reliability of the financial services and markets sector; (e) an asset that: (i) is owned or operated by an Australian body corporate that holds a benchmark administrator licence; and (ii) is used in connection with the administration of a significant financial benchmark, that, in accordance with subsection (4), is critical to the security and reliability of the financial services and markets sector; (f) an asset that: (i) is owned or operated by an associated entity of an Australian body corporate that holds a benchmark administrator licence; and (ii) is used in connection with the administration of a significant financial benchmark, that, in accordance with subsection (4), is critical to the security and reliability of the financial services and markets sector; (g) an asset that: (i) is owned or operated by an Australian body corporate that holds an Australian derivative trade repository licence; and

	(ii) is used in connection with the operation of a derivative trade repository, that, in accordance with subsection (5), is critical to the security and reliability of the financial services and markets sector; (h) an asset that: (i) is owned or operated by an associated entity of an Australian body corporate that holds an Australian derivative trade repository licence; and (ii) is used in connection with the operation of a derivative trade repository, that, in accordance with subsection (5), is critical to the security and reliability of the financial services and markets sector; (i) an asset that is used in connection with the operation of a payment system, that, in accordance with subsection (6), is critical to the security and reliability of the financial services and markets sector. Note: The rules may prescribe that a specified critical financial market infrastructure asset is not a critical infrastructure asset (see section 9). (2)For the purposes of paragraphs (1)(a) and (b), the rules may prescribe: (a) specified financial markets that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for a financial market to be critical to the security and reliability of the financial services and markets sector. (3)For the purposes of paragraphs (1)(c) and (d), the rules may prescribe: (a) specified clearing and settlement facilities that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for a clearing and settlement facility to be critical to the security and reliability of the financial services and markets sector. (4)For the purposes of paragraphs (1)(e) and (f), the rules may prescribe: (a) specified significant financial benchmarks that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for a significant financial benchmark to be critical to the security and reliability of the financial services and markets sector. (5)For the purposes of paragraphs (1)(g) and (h), the rules may prescribe: (a) specified derivative trade repositories that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for a derivative trade repository to be critical to the security and reliability of the financial services and markets sector. (6)For the purposes of paragraph (1)(i), the rules may prescribe: (a) specified payment systems that are critical to the security and reliability of the financial services and markets sector; or (b) requirements for a payment system to be critical to the security and reliability of the financial services and markets sector. (7)For the purposes of this section, ***Australian body corporate*** means a body corporate that is incorporated in Australia.
Critical food and grocery asset	(1)An asset is a ***critical food and grocery asset*** if it 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) a critical supermarket retailer, in accordance with subsection (2); or (ii) a critical food wholesaler, in accordance with subsection (3); or (iii) a critical grocery wholesaler, in accordance with subsection (4). Note: The rules may prescribe that a specified critical food and grocery asset is not a critical infrastructure asset (see section 9). (2)For the purposes of subparagraph (1)(b)(i), the rules may prescribe: (a) specified entities that are critical supermarket retailers; or (b) requirements for an entity to be a critical supermarket retailer. (3)For the purposes of subparagraph (1)(b)(ii), the rules may prescribe: (a) specified entities that are critical food wholesalers; or (b) requirements for an entity to be a critical food wholesaler. (4)For the purposes of subparagraph (1)(b)(iii), the rules may prescribe: (a) specified entities that are critical grocery wholesalers; or (b) requirements for an entity to be a critical grocery wholesaler.
Critical hospital	Critical hospital means a hospital that has a general intensive care unit.
Critical education asset	Critical education asset means a university that is owned or operated by an entity that is registered in the Australian university category of the National Register of Higher Education Providers.
Critical space technology asset	Bill **does not** insert a specific definition of a *critical space technology asset* as entities would be captured as carriers and carriage service providers under the TSSR.
Critical Port	An asset is a critical port if it is land that forms part of any of the following security regulated ports: (a) Broome Port; (b) Port Adelaide; (c) Port of Brisbane; (d) Port of Cairns; (e) Port of Christmas Island; (f) Port of Dampier; (g) Port of Darwin; (h) Port of Eden; (i) Port of Fremantle; (j) Port of Geelong; (k) Port of Gladstone; (l) Port of Hay Point; (m) Port of Hobart; (n) Port of Melbourne; (o) Port of Newcastle; (p) Port of Port Botany; (q) Port of Port Hedland; (r) Port of Rockhampton; (s) Port of Sydney Harbour; (t) Port of Townsville; (u) A security regulated port prescribed by the rules for the purposes of this paragraph.

Critical Aviation Asset	(a) an asset that: (i)is used in connection with the provision of an air service; and (ii)is owned or operated by an aircraft operator; or (b) an asset that: (i)is used in connection with the provision of an air service; and (ii)is owned or operated by a regulated air cargo agent; or (c)an asset that is used by an airport operator in connection with the operation of an airport. (1)
Critical Freight Infrastructure Asset	(1)An asset is a ***critical freight infrastructure asset*** if it is any of the following: (a) a road network that, in accordance with subsection (2), functions as a critical corridor for the transportation of goods between: (i) 2 States; or (ii) a State and a Territory; or (iii) 2 Territories; or (iv) 2 regional centres; (b) a rail network, that, in accordance with subsection (3), functions as a critical corridor for the transportation of goods between: (i) 2 States; or (ii) a State and a Territory; or (iii) 2 Territories; or (iv) 2 regional centres; (c) an intermodal transfer facility, that, in accordance with subsection (4), is critical to the transportation of goods between: (i) 2 States; or (ii) a State and a Territory; or (iii) 2 Territories; or (iv) 2 regional centres. Note: The rules may prescribe that a specified critical freight infrastructure asset is not a critical infrastructure asset (see section 9). (2)For the purposes of paragraph (1)(a), the rules may prescribe: (a) specified road networks that function as a critical corridor for the transportation of goods between: (i) 2 States; or (ii) a State and a Territory; or (iii) 2 Territories; or (iv) 2 regional centres; or (b) requirements for a road network to function as a critical corridor for the transportation of goods between: (i) 2 States; or (ii) a State and a Territory; or (iii) 2 Territories; or (iv) 2 regional centres. (3)For the purposes of paragraph (1)(b), the rules may prescribe: (a) specified rail networks that function as a critical corridor for the transportation of goods between:

	(i) 2 States; or (ii) a State and a Territory; or (iii) 2 Territories; or (iv) 2 regional centres; or (b) requirements for a rail network to function as a critical corridor for the transportation of goods between: (i) 2 States; or (ii) a State and a Territory; or (iii) 2 Territories; or (iv) 2 regional centres. (4)For the purposes of paragraph (1)(c), the rules may prescribe: (a) specified intermodal transfer facilities that are critical to the transportation of goods between: (i) 2 States; or (ii) a State and a Territory; or (iii) 2 Territories; or (iv) 2 regional centres; or (b) requirements for an intermodal transfer facility to be critical to the transportation of goods between: (i) 2 States; or (ii) a State and a Territory; or (iii) 2 Territories; or (iv) 2 regional centres. (5)For the purposes of this section, ***road network*** includes a part of a road network. (6)For the purposes of this section, ***rail network*** includes a part of a rail network.
Critical Freight Services Asset	(1)An asset is a ***critical freight services asset*** if it is a network that is used by an entity carrying on a business, that, in accordance with subsection (2), is critical to the transportation of goods by any or all of the following: (a) road; (b) rail; (c) inland waters; (d) sea. Note: The rules may prescribe that a specified critical freight services asset is not a critical infrastructure asset (see section 9). (2)For the purposes of subsection (1), the rules may prescribe: (a) specified businesses that are critical to the transportation of goods by any or all of the following: (i) road; (ii) rail; (iii) inland waters; (iv) sea; or (b) requirements for a business to be critical to the transportation of goods by any or all of the following: (i) road;

	(ii) rail; (iii) inland waters; (iv) sea.
Critical Public Transport Asset	Critical public transport asset means a public transport network or system that: (a) is managed by a single entity; and (b) is capable of handling at least 5 million passenger journeys per month.
Critical electricity asset	(1) An asset is a critical electricity asset if it is: (a) a network, system, or interconnector, for the transmission or distribution of electricity to ultimately service at least 100,000 customers; or (b) an electricity generation station that is critical to ensuring the security and reliability of electricity networks or electricity systems in a State or Territory, in accordance with subsection (2). (2) For the purposes of paragraph (1)(b), the rules may prescribe requirements for an electricity generation station to be critical to ensuring the security and reliability of electricity networks or electricity systems in a particular State or Territory.
Critical gas asset	(1) An asset is a critical gas asset if it is any of the following: (a) a gas processing facility that has a capacity of at least 300 terajoules per day or any other capacity prescribed by the rules; (b) a gas storage facility that has a maximum daily quantity of at least 75 terajoules per day or any other quantity prescribed by the rules; (c) 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; (d) a gas transmission pipeline that is critical to ensuring the security and reliability of a gas market, in accordance with subsection (2). (2) For the purposes of paragraph (1)(d), the rules may prescribe: (a) specified gas transmission pipelines that are critical to ensuring the security and reliability of a gas market; or (b) requirements for a gas transmission pipeline to be critical to ensuring the security and reliability of a gas market.
Critical liquid fuel asset	(1)An asset is a ***critical liquid fuel asset*** if it is any of the following: (a) a liquid fuel refinery that is critical to ensuring the security and reliability of a liquid fuel market, in accordance with subsection (2); (b) a liquid fuel pipeline that is critical to ensuring the security and reliability of a liquid fuel market, in accordance with subsection (3); (c) a liquid fuel storage facility that is critical to ensuring the security and reliability of a liquid fuel market, in accordance with subsection (4). Note: The rules may prescribe that a specified critical liquid fuel asset is not a critical infrastructure asset (see section 9). (2)For the purposes of paragraph (1)(a), the rules may prescribe: (a) specified liquid fuel refineries that are critical to ensuring the security and reliability of a liquid fuel market; or (b) requirements for a liquid fuel refinery to be critical to ensuring the security and reliability of a liquid fuel market. (3)For the purposes of paragraph (1)(b), the rules may prescribe: (a) specified liquid fuel pipelines that are critical to ensuring the security and reliability of a liquid fuel market; or

	(b) requirements for a liquid fuel pipeline to be critical to ensuring the security and reliability of a liquid fuel market. (4)For the purposes of paragraph (1)(c), the rules may prescribe: (a) specified liquid fuel storage facilities that are critical to ensuring the security and reliability of a liquid fuel market; or (b) requirements for a liquid fuel storage facility to be critical to ensuring the security and reliability of a liquid fuel market.
Critical energy market operator asset	Critical energy market operator asset means an asset that: (a) is owned or operated by: (i) Australian Energy Market Operator Limited (ACN 072 010 327); or (ii) Power and Water Corporation; or (iii) Regional Power Corporation; or (iv) Electricity Networks Corporation; and (b) is used in connection with the operation of an energy market or system; and (c) is critical to ensuring the security and reliability of an energy market; but does not include: (d) a critical electricity asset; or (e) a critical gas asset; or (f) a critical liquid fuel asset.
Critical water asset	critical water asset means one or more water or sewerage systems or networks that: (a) are managed by a single water utility; and (b) ultimately deliver services to at least 100,000 water connections or 100,000 sewerage connections.