Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE CENTRE

# Protecting Critical Infrastructure and Systems of National Significance

Consultation Paper
August 2020

# Contents

# Who should read this paper?

All Australians rely on critical infrastructure to deliver essential services that are crucial to our way of life, such as electricity, communications, transport and banking.

As such, we encourage all Australians to take an active interest in ensuring that Australia's approach to protecting critical infrastructure is fit for purpose for the modern age.

From a critical infrastructure perspective, we are especially keen to hear from the following sectors, given their fundamental importance to our economy, security and sovereignty:

- Banking and finance
- Communications
- Data and the Cloud
- Defence industry
- Education, research and innovation
- Energy
- Food and grocery
- Health
- Space
- Transport
- Water.

# Overview

## The Australian Government is committed to protecting the essential services all Australians rely on by uplifting the security and resilience of critical infrastructure.

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

A range of hazards have the potential to significantly compromise the supply of essential services across Australia; physical, personnel and cyber security are all increasingly interrelated. Recent incidents such as compromises of the Australian parliamentary network, university networks and key corporate entities, natural disasters and the impacts of COVID-19 illustrate that threats to the operation of Australia's critical infrastructure entities continue to be significant.

We must work together now to ensure Australia's security practices, policies and laws bolster the security and resilience of our critical infrastructure and position us to act in any future emergency. We need a better shared understanding of the threats we face and how we can combat them. Together, owners and operators of critical infrastructure, academia and all levels of government must collectively take steps to protect Australians from an attack and other disruptions.

Accordingly, Government will introduce an enhanced regulatory framework, building on existing requirements under the *Security of Critical Infrastructure Act 2018* (the Act). This will include:

- a positive security obligation for critical infrastructure entities, supported by sector-specific requirements;
- enhanced cyber security obligations for those entities most important to the nation; and
- Government assistance to entities in response to significant cyber attacks on Australian systems.

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

The Government's commitment to the continued prosperity of our economy and businesses is unwavering. The impacts of recent events only reinforce the need for collaboration between and across critical infrastructure sectors and Government to protect our economy, security and sovereignty.

At the same time, Government recognises the additional economic challenges facing many sectors and entities in the wake of the COVID-19 pandemic. The outcome we seek is clear - we want to work in partnership to develop proportionate requirements that strike a balance between uplifting security, and ensuring businesses remain viable and services remain sustainable, accessible and affordable. An uplift in security and resilience across critical infrastructure sectors will mean that all businesses will benefit from strengthened protections to the networks, systems and services we all depend on.

We want to hear from you – owners and operators of critical infrastructure, state and territory governments, academia and the Australian public – to contribute to the design of this framework to deliver a real and meaningful uplift to critical infrastructure security and resilience, while minimising economic impact.

# Where we are now

## The interconnected nature of our critical infrastructure means that compromise in one essential function can have a domino effect that degrades or disrupts others.

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

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

At its most extreme, such catastrophic disruption could cause loss of life. Recent events, particularly COVID-19, have demonstrated how threats can have flow on effects across multiple sectors. A deliberate cyber attack could have farther-reaching, more rapid and less visible causes and effects.

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

- Over the last two years, we have seen several cyber attacks in Australia that have targeted the Federal Parliamentary Network, 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.

While the Australian Government and industry continually work on responses to incidents impacting our critical infrastructure, there is scope to be more proactive and take preparatory activities to understand, mitigate and prevent threats. A cohesive partnership between the Government and industry, especially through sharing of technical expertise, is a desirable end state. Collective action now will place Australia in the best position to combat both foreseeable and emerging risks. The enhanced framework will meet this need, supported by proportionate sector-specific standards.

# What you have told us

The Department of Home Affairs values its ongoing engagement with critical infrastructure entities. Mechanisms like the Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN) are important forums for cross sector dialogue, facilitating ongoing feedback on the security environment facing us all. As outlined in the Cyber Security Strategy 2020, through consultation the Australian 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 Discussion Paper.

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.[1] Timely and actionable information sharing was identified as a critical gap.

We heard that Government's role in addressing these threats and gaps should start by:

- driving an uplift in resilience across sectors through regulation;
- clarifying roles, responsibilities and expectations; and
- using its unique capabilities to address serious cyber threats to Australia.

We heard that Government also needs to explain how security risks are managed, how responsibilities are shared across the economy, and how Government and critical infrastructure entities can work together to protect Australia's critical infrastructure from sophisticated threats.

Consultations highlighted that the Australian public looks to both Government and critical infrastructure to secure the delivery of essential services. We need to collaborate and prepare ahead of time, so everyone knows what their role is and what they need to do in an emergency. To do this, Government and critical infrastructure entities need the right processes, authorisations and powers in place to respond rapidly and decisively.

The framework set out in this Consultation Paper is put forward as a starting proposition to position all levels of government – Commonwealth, state, territory and local – and critical infrastructure to identify levels of entity criticality, appropriately minimise the likelihood and impact of significant incidents occurring, and to respond where necessary in the national interest.

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

# What we have learned

This feedback complements the greater understanding of the interdependencies between critical infrastructure sectors, and supply chains, enabled by the Act and Government's longstanding engagement with critical infrastructure owners and operators.

Since July 2018, the Act requires specific critical infrastructure owners and operators to provide ownership and operational information to the Australian Government. Some key insights include:

- Enhanced understanding of the ultimate ownership of entities.
- Improved visibility of entities' supply chain and outsourcing arrangements, including for storage of sensitive operational data.
- Greater understanding of associated entities and links to other companies, enhancing the Government's overall understanding of our critical infrastructure sectors and potential vulnerabilities.
- Identification of a range of common services being used by multiple entities, such as shared information technology service providers or shared control systems and reliance on offshore operational technology providers and subject matter expertise.

These key insights have highlighted a range of legitimate business practices that may have security implications. Enhancing the regulatory environment will help ensure that businesses, while continuing to operate in a global, networked environment, have security and resilience at the forefront of their planning.

In addition, the Act currently covers specific entities in the electricity, gas, water and ports sectors. As Government has improved visibility of how interconnected Australia's critical infrastructure is, this has highlighted a need to consider expanding the types of critical infrastructure entities subject to the Act to include more critical infrastructure entities in a wider range of sectors.

# Where we need to be – an enhanced critical infrastructure framework

## Objective of the enhanced framework

The primary objective of the proposed enhanced framework is to **protect Australia's critical infrastructure** from all hazards, including the dynamic and potentially catastrophic cascading threats enabled by cyber attacks.

The enhanced framework outlines a need for an uplift in security and resilience in **all critical infrastructure sectors**, combined with better identification and sharing of threats in order to make Australia's critical infrastructure – whether industry or government owned and operated – more resilient and secure. This approach will prioritise acting ahead of an incident wherever possible.

However, we recognise that **one size does not fit all**. We need to balance consistent objectives that provide a baseline of **cyber, physical, personnel and supply chain protections** across all sectors, with the reality that there are sector specific differences in human and financial resources, technology, threats, existing standards and maturity, to name a few. This is why the framework is proposed to be built around principles-based obligations that will sit in legislation, and underpinned by sector-specific guidance and advice, proportionate to the risks and circumstances faced by each sector. Furthermore, legislative requirements will remain proportionate and collaborative, while avoiding inconsistent application of regulations putting entities at a commercial disadvantage.

To ensure these security outcomes, we recognise that uplift is required in all critical infrastructure sectors and that Government must be an exemplar. Accordingly, we will continue to work towards enhanced security for government and democratic institutions, and will work within the Commonwealth and with states and territories to identify the most appropriate mechanisms to ensure governments are held to the same standards as owners and operators of critical infrastructure.

To respond to Australia's evolving threat environment, we need to build a partnership that benefits all critical infrastructure, as well as the Australian public. It is not enough for owners and operators to uplift their resilience. Government should use its unique position and resources to share aggregated threat information, work with critical infrastructure entities of all levels of maturity to build their capability, and empower entities to appropriately protect themselves when faced with a serious threat.

# Features of the enhanced framework

Government has agreed that the proposed enhanced framework will apply to an expanded set of critical infrastructure sectors, comprising of three key elements:

1. **Positive Security Obligation,** including:
    a. set and enforced baseline protections against all hazards for critical infrastructure and systems, implemented through sector-specific standards proportionate to risk.
2. **Enhanced cyber security obligations** that establish:
    a. the ability for Government to request information to contribute to a near real-time national threat picture;
    b. owner and operator participation in preparatory activities with Government; and
    c. the co-development of a scenario based 'playbook' that sets out response arrangements.
3. **Government assistance for entities** that are the target or victim of a cyber attack, through the establishment of a Government capability and authorities to disrupt and respond to threats in an emergency.

These three initiatives will be underpinned by an **enhanced Government-industry partnership** across all hazards that, among other measures, will focus on:

- reinvigorating and expanding existing engagement platforms and strategies;
- improving coordination across government to provide appropriately classified whole-of-government threat assessments and briefings to entities;
- co-designing best practice guidance with critical infrastructure entities, state, territory and Australian Government partners and regulators, as well as international partners; and
- delivering a comprehensive, multi-year program of workshops, exercises, information sharing sessions and assessments to complement and inform sector and sub-sector based assessments.

We recognise that there will be a regulatory impost in delivering these reforms. We will work with critical infrastructure entities to ensure that these reforms are developed and implemented in a manner that secures appropriate outcomes without imposing unnecessary or disproportionate regulatory burden, in accordance with guidance from the Department of the Prime Minister and Cabinet's Office of Best Practice Regulation.

# What do we want your views on?

Noting the above agreed features of the framework, we want your views on the detail that sits underneath each of these elements and how we can work together to ensure they are best designed and delivered.

We have asked a series of questions throughout the paper to help frame your input.

# Who will the enhanced framework apply to?

The Australian Government's Critical Infrastructure Resilience Strategy currently defines critical infrastructure as:

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

Within that broad definition of critical infrastructure, the Act currently places regulatory obligations on specific entities in the **electricity, gas, water and maritime ports sectors**. However, entities across all critical infrastructure sectors are facing increasing threats and may require enhanced protections.

These reforms will bring proportionate security obligations to:

- Banking and finance
- Communications
- Data and the Cloud
- Defence industry
- Education, research and innovation
- Energy
- Food and grocery
- Health
- Space
- Transport
- Water.

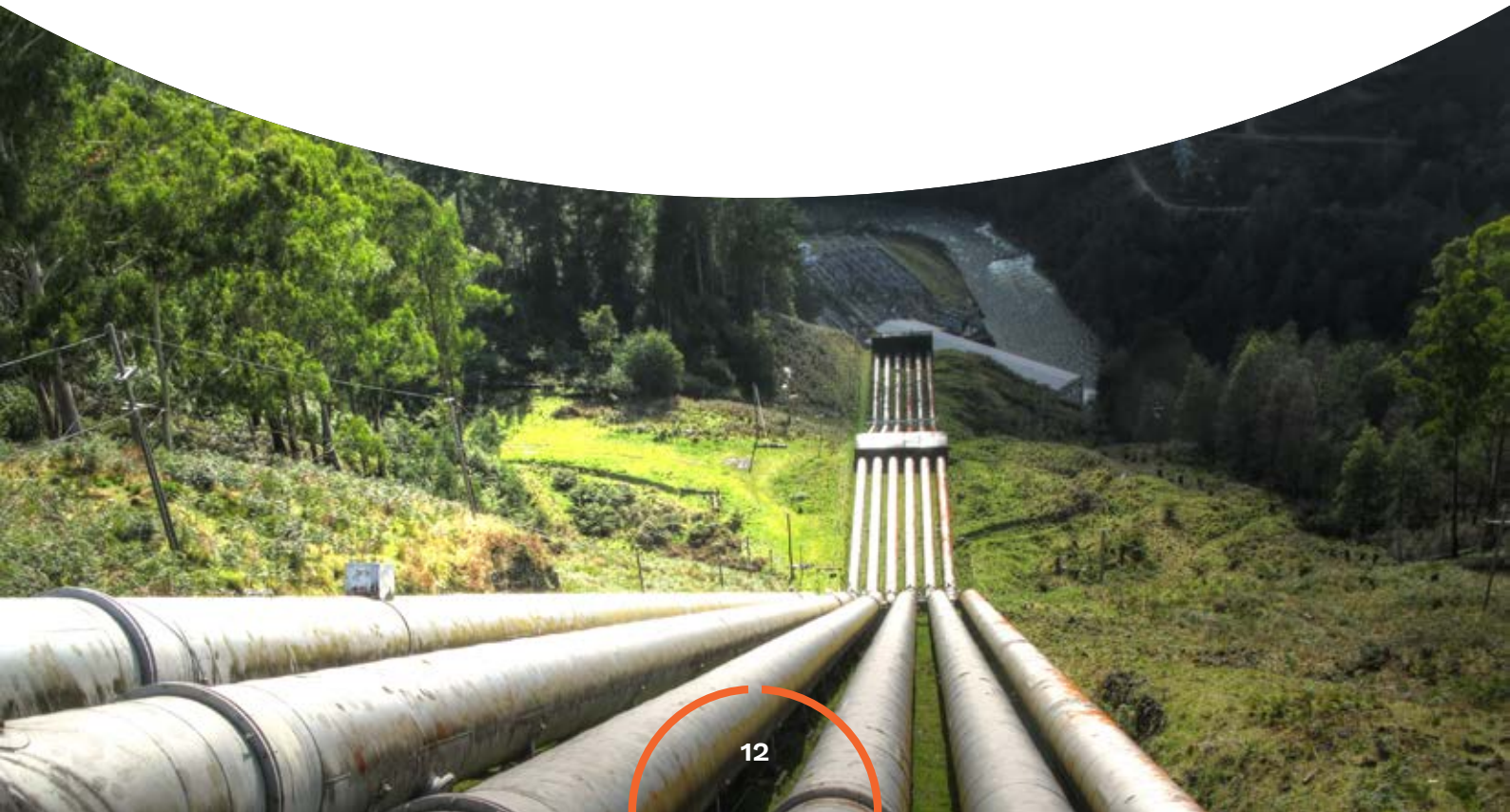
[2] See, the Australian Government's *Critical Infrastructure Resilience Strategy Plan (2015)*. See also, https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf; https://www.legislation.gov.au/Details/C2018A00029

The services that these sectors provide are crucial to Australia's economy, security and sovereignty. It is essential that critical infrastructure entities within these sectors take a proactive approach to security and resilience. Mature sectors will benefit from an uplift in their supply chain, as well as the networks and systems that they depend on.

Government will work in partnership with critical infrastructure entities to ensure the new requirements **build on and do not duplicate existing regulatory frameworks**. This approach recognises that 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. By focusing on outcomes, the new framework will ensure consistent security standards across all sectors without unnecessary regulatory impost.

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

Australians expect all critical infrastructure to secure the essential services they rely on, regardless of ownership. We all have an obligation to meet this standard. We will work with states and territories to ensure all critical infrastructure is held to the same standards, regardless of ownership.

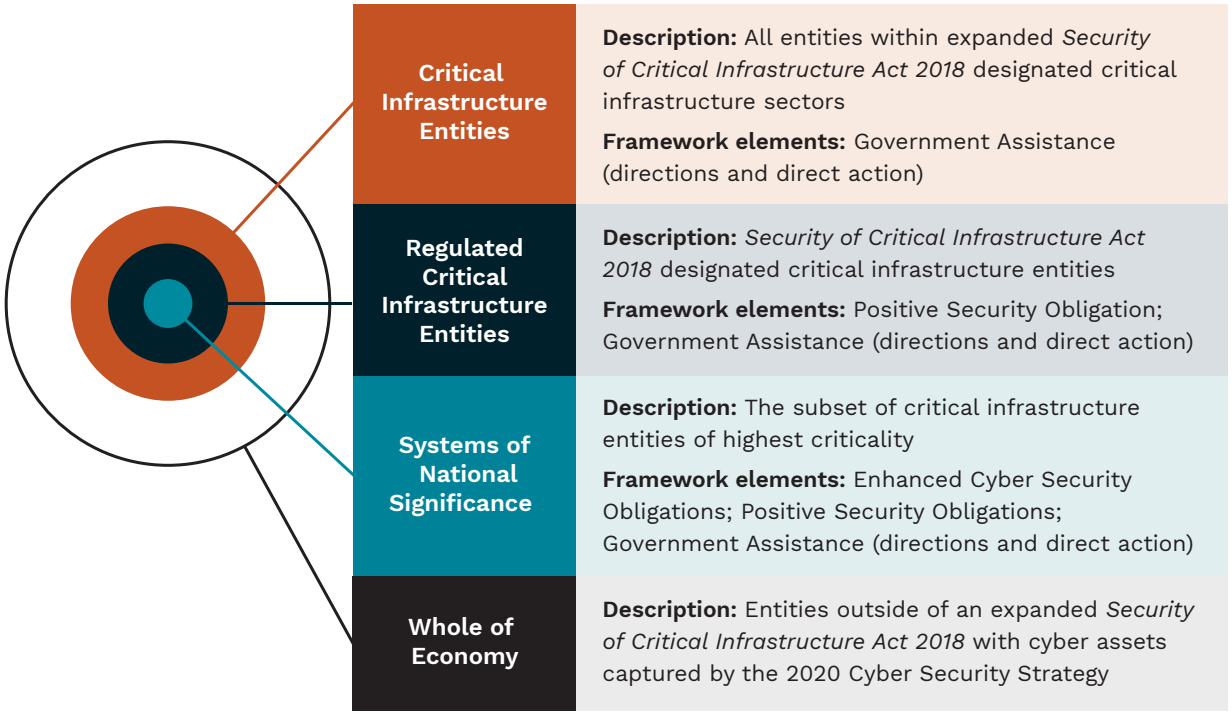


# Which entities will be covered?

A key principle underpinning the design of the reforms is that to achieve maximum impact Australia's critical infrastructure and governments should work together to **apply resources** to protect the systems and entities that are most critical to Australia's economy, security and sovereignty. This includes ensuring reasonable and appropriate regulatory coverage.

The reforms include broad levels of categorisation that will set out obligations and determine how Government will engage with different owners and operators. These are outlined in Figure 1.

**Figure 1:** Classes of Entities and Relevant Elements of the Framework – Entity Level




As the above figure indicates, only a subset of entities will be subject to all parts of the reforms.

We need to work with you to map and identify what should become a 'critical infrastructure entity', a 'regulated critical infrastructure entity' subject to the Positive Security Obligation and the small subset of entities that are the **most important** to the nation—which we will refer to as '*Systems of National Significance*'—additionally subject to the Enhanced Cyber Security Obligations. To do this, we will consider:

- **Interdependency with other functions**, including: the potential for a domino effect if the function were compromised; and vulnerabilities within and between systems and networks.
- **The consequence of compromise** to the entity, including: immediate threat to life; sensitivity of data; and broader impacts on economy, security, sovereignty and the well-being of Australians.

The mapping process will be conducted using criteria to be developed on a sector-specific basis taking into account:

- an **entity's internal characteristics** including for example the nature and/or volume of a particular product or service the entity supplies; and
- the **characteristics of its external operating environment** including for example its customers, network interdependency, redundancy and resilience to hazards.

In developing the criteria for assessing which entities will be covered by the reforms we will be guided by the principles of simplicity, transparency, accuracy and stabillity.

The proposed reforms will be focused at the owner and operator level, not at a specific piece of technology. This ensures that owners and operators' interconnected assets are protected from cascading failures, and avoids creating vulnerabilities in one area by disproportionately focusing efforts on protecting others.

We will identify and map owners and operators of critical infrastructure through the public consultation process. This Government-critical infrastructure collaboration will include workshops with entities and peak bodies, invitations from Government to respond to surveys and engagement with sector regulators and lead policy departments.

## Call for views

1. Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?
2. Do you think the current definition of Critical Infrastructure is still fit for purpose?
3. Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?
4. What are the common threats you routinely prepare for and those you have faced/ experienced as a business?
5. How should criticality be assessed to ensure the most important entities are covered by the framework?
6. Which entities would you expect to be owners and operators of systems of national significance?

# Government-Critical Infrastructure collaboration to support uplift

## Ongoing collaboration and engagement with critical infrastructure is vital to uplifting critical infrastructure security and resilience.

Australia is more resilient when we all work together, and the Government is committed to building on the strength of this partnership, and investing in its ongoing success.

### Working together

The Department of Home Affairs will seek to enhance and integrate Government's existing critical infrastructure education, communication and engagement activities, through a reinvigorated TISN and updated Critical Infrastructure Resilience Strategy. This may include a range of activities to improve critical infrastructure and Government's engagement and collective understanding of risk within and across sectors, such as:

- Co-designing **best practice guidance** with entities, government and international partners.
- Improving coordination across Government to provide appropriately classified whole-of-government all hazard **threat assessments and briefings** to entities.
- Using Structured Analytical Techniques such as all hazards scenario planning to improve understanding of risk within and across sectors.
- Drawing on expertise across Government, offering participants **individualised vulnerability assessments**.
- Enhancing Government's existing **research, analysis and evaluation capabilities** to enable ongoing improvements to risk management. This may include dependency modelling, research into evolving risk management practice, and collaboration with academia.
- Ensuring that the **Boards of critical infrastructure entities have visibility** of, and are responsible for planning and actively managing security and resilience.
- Introducing a two-way **industry-government secondment program** to deepen collaboration.
- Improving Ministerial visibility by reporting annually on work undertaken through this partnership.

# Call for views

7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?
8. What might this new TISN model look like, and what entities should be included?
9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?

# Initiative 1: Positive Security Obligation

The Positive Security Obligation (PSO) will propose a set of principles-based outcomes across Australia's critical infrastructure sectors to protect entities from all-hazards.

As outlined in Figure 1, the PSO will apply to entities designated as '*Regulated Critical Infrastructure Entities*' and owners and operators of '*Systems of National Significance*'.

We recognise there already exists a range of mechanisms to manage certain hazards and we do not propose to duplicate or replace these. Instead, throughout this process we want to work with you to identify those existing mechanisms and where necessary, build on them to deliver a more consistent approach to managing risk across all sectors.

We want to work with you to identify regulators for your critical infrastructure sector and design the detail around how critical infrastructure entities in your sector can meet their PSO obligations.

## Principles-based outcomes

We want to work with critical infrastructure entities to clearly define the high level, sector-agnostic principles that will form the basis for the PSO. We consider that at a minimum, owners and operators of critical infrastructure should be legally obliged to manage risks that may impact business continuity and Australia's economy, security and sovereignty, by meeting the following PSO principles-based outcomes.

### 1. Identify and understand risks

Entities will have a responsibility to take an all-hazards approach when identifying and understanding risks. This will consider both natural and human induced hazards. 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.

### 2. Mitigate risks to prevent incidents

Entities will be required to have appropriate risk mitigations in place to manage identified risks applicable to their sector. Risk mitigation should consider both proactive risk management as well as having processes in place: to detect and respond to threats as they are being realised; and plan for disasters and have a way to lessen the negative impact were it to actually occur. The regulated entity will be responsible for engaging with the regulator to ensure that identified risks and proposed mitigations are proportionate to the risks, while also considering the business, societal and economic impacts.

### 3. Minimise the impact of realised incidents

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

### 4. Effective governance

Entities will be required to have appropriate risk management oversight and responsibilities in place, including evaluation and testing. This will involve strong governance with clear lines of accountability, demonstrated comprehensive planning, and a robust assurance and review process in place that is proportionate to the identified risks. Compliance will be assessed by the relevant regulator noting that what is appropriate may be unique to each entity. Regulators will focus on outcomes and seek to avoid compliance burden.

# Security Obligations

We consider that the new framework should clearly set out in legislation the high-level security obligations that critical infrastructure entities should meet. At a minimum, we consider these to be:

### Physical security

Critical infrastructure entities will be required to protect their systems and networks by considering and mitigating natural, and human induced threats. This may include:

- Implementing proportionate physical security measures that lessen the risk of harm to people, information and physical asset resources being made unlawfully inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.
- Integrating protective security into the process of planning, selecting, designing and modifying facilities for the protection of people, information and physical assets.
- Securing physical spaces where sensitive information and assets are used, transmitted, stored or discussed.

### Cyber security

Critical infrastructure entities will protect their systems and information from cyber threats. This may include:

- Identifying and assessing sensitive information and implementing proportionate controls.
- Understanding access to an entity's sensitive information, with need to know principles applied.
- Endeavouring to safeguard information from common and emerging cyber threats and adhering to best practice guidelines.
- Implementing robust security measures during all stages of ICT systems development.
- Aiming to ensure systems and personnel can detect, understand and respond to cyber security incidents.

### Personnel security

Critical infrastructure entities will implement policies and procedures which seek to mitigate the risk of employees (insider threats) exploiting their legitimate access to an organisation's assets for unauthorised purposes. This may include:

- Ensuring only suitable employees and contractors access the entity's resources and are aware of, and meet, appropriate standards of conduct.
- Assessing and managing the ongoing suitability of its personnel to access resources throughout their engagement.
- Promoting a positive and collaborative security culture of continual improvement and engagement across sectors, ensuring lessons learnt are shared.

### Supply chain security

Critical infrastructure entities will protect their operations by understanding supply chain risk. Supply chains can be compromised or disrupted from a variety of natural or man-made activities.[3]

## Call for views

10. Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?
11. Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?
12. Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?
13. What costs would organisations take on to meet these new obligations?
14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

[3] Australian Cyber Security Centre's *Cyber Supply Chain Risk Management Practitioner Guide* (2020) provide clear guidance on best practice supply chain management.

# Regulators

In recognition that one size does not fit all and that there are various standards and requirements already in place for some sectors, we will work with critical infrastructure entities to identify the most appropriate regulator for each sector.

Consultation will not end with establishing the enhanced legislative framework. Regulators will continue to work with entities to co-design sector-specific requirements and guidance to ensure the PSO is applied, taking into account the needs and capabilities of each sector. Regulators will also have a role in monitoring compliance and enforcing these obligations.

**Figure 2** outlines a process map of this model.

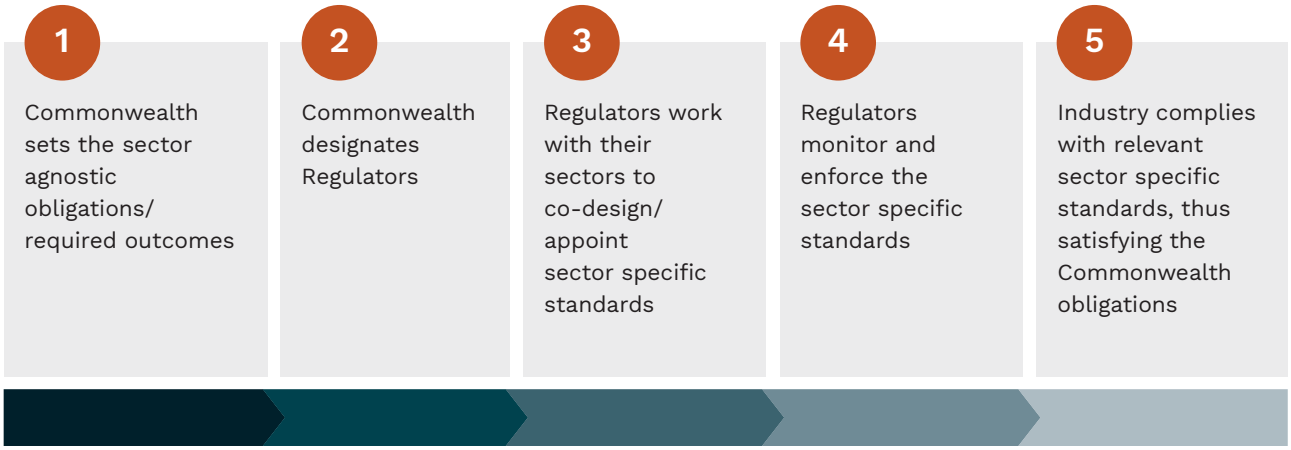
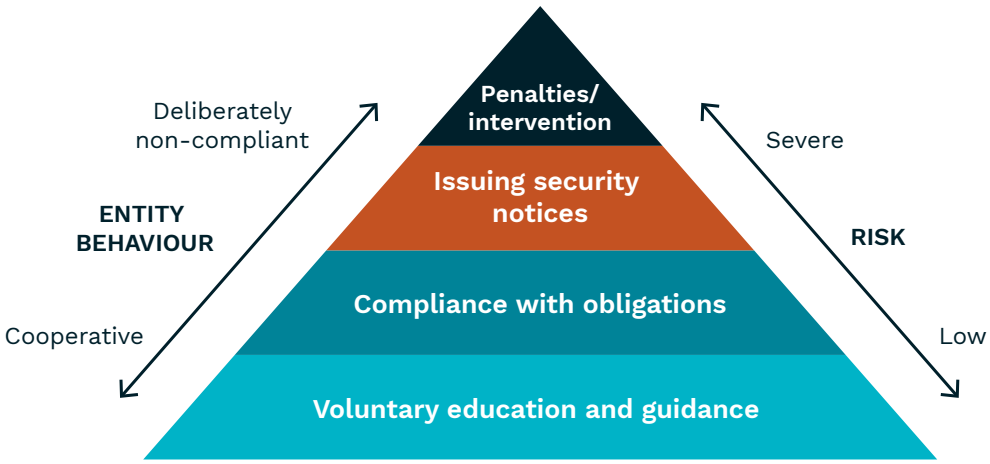



**Figure 2.** Regulatory Model

Regulators will adopt a risk based approach in developing and enforcing the PSO (see Figure 3) that emphasises education and guidance in the first instance. Government considers that incident reporting, including actions taken to address those incidents, will be an essential component of this framework. Regulators should also consider the potential impact of PSO requirements and seek to minimise their economic and operational impact on businesses.




| Voluntary education and guidance | Compliance with obligations | Issuing security notices | Penalties and intervention |
|---|---|---|---|
| • Educating entities on best practice<br>• Ensuring obligations are understood<br>• Maintaining two-way discussions to build understanding<br>• Promotion of best practice security culture | • Review and assessment of Security Plans<br>• Ability to issue reasonable requests for information and inspect | • Issuing security notices that would need to be taken into account | • Intervene and issue directives<br>• Issuing penalties |

**Engagement** **Enforcement**

**Figure 3:** PSO Regulatory Approach Model

## Education and Guidance

Regulators will be responsible for educating and guiding entities towards best practice security management wherever possible. This will include:

- educating entities and ensuring their legislative and administrative obligations are understood; and
- developing and maintaining strong links with entities to promote ongoing best practice.

## Compliance and enforcement

Regulators will build an understanding of entities' compliance through an agreed, Board-approved (or equivalent level) reporting mechanism which may be submitted annually or as otherwise agreed. This recognises that the Board (or equivalent) of the regulated entity is ultimately responsible for ensuring that risk is managed appropriately.

Guided by the PSO principles, the agreed form of reporting should demonstrate comprehensive risk identification and ensure appropriate risk mitigations with clear lines of accountability are in place. Reporting should also address any issues identified for action by the regulator or security incidents that have occurred in the preceding year and actions taken to address those incidents.

Regulators will enforce the PSO requirements through flexible administrative measures and graduated enforcement powers (set out in the Act or enabling legislation, in addition to existing powers they may hold). Compliance and enforcement action (in line with the *Regulatory Powers Act 2014*) would include:

- overseeing compliance with the legislative obligations (notwithstanding other compliance powers, evidenced through reporting to the regulator and timely responses to security notices);
- the ability to issue reasonable requests for access to information and inspection and audit powers;
- issuing security notices that entities would need to take into account and evidence in their reporting as part of meeting their obligations;
- provide detailed guidance on how to achieve compliance;
- the ability to intervene and issue directions in cases where there are significant national security concerns that cannot be addressed through other means; and
- the ability to issue penalties for non-compliance.

# Call for views

15. Would the proposed regulatory model avoid duplication with existing oversight requirements?
16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?
17. Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?
18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?
19. How can Government better support critical infrastructure entities in managing their security risks?
20. In the AusCheck scheme, potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?
21. Do you have any other comments you would like to make regarding the PSO?

# Initiative 2: Enhanced Cyber Security Obligations

The PSO sets a proposed set of outcomes to increase the overall security of the critical infrastructure. In addition, we are seeking your views on measures to help protect Australia's most critical entities prepare for cyber attacks. These will only apply to particularly critical entities where there is a need to build an active partnership based on near-real time information to better understand and address threats. Through the mapping process, these entities will be identified as **most important** – our systems of national significance.

## Situational awareness

Improving Australia's situational awareness will strengthen the ability of owners and operators of systems of national significance to take action to reduce the risk and impact of a significant cyber attack against our systems of national significance. During consultation on Australia's *2020 Cyber Security Strategy*, we heard that Government needs to work with critical infrastructure to better understand cyber threats.

Government is looking to establish a capability to facilitate information sharing with relevant owners and operators – whether industry or Government. We will work to develop a near real-time national threat picture, which will require information from a variety of sources, including:

- industry and commercial partnerships;
- incident reporting;
- cross-sectoral dependency projects;
- open source information; and
- Government intelligence and international feeds.

Working together is essential to developing a near real-time threat picture. We will draw on both Government and entity insights to develop and share a comprehensive view of cyber threats that is mutually beneficial.

A near real-time threat picture, including intelligence insights and trends, will empower owners and operators of systems of national significance to take appropriate and timely action on their own systems. It will also provide the Government with an aggregated threat picture and comprehensive understanding of the risks to critical infrastructure. This will better inform both proactive and reactive cyber response options.

**Note:** Information shared by Government through this initiative will be information about networks and systems, **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.

Entity information will be requested by Government on a voluntary basis in the first instance (supported by appropriate agreements), in order to test the concept, build the capability and ensure information being shared meets the needs of owners and operators of systems of national significance.

In the longer term, owners and operators of systems of national significance will be obligated (under amendments to the Act) **to provide information about networks and systems** to contribute to this threat picture if requested. When a request is issued, it will include the format the information is required in (up to and including near real-time), as well as a specified timeframe to work with the Government to provide the information. At present, we do not anticipate that all owners and operators of systems of national significance will be requested to provide such information.

Some entities will already have a mature capability allowing them to voluntarily provide Government with the information required and receive actionable, aggregated information in return. Some entities will be at the other end of the maturity spectrum and may need to build their capability first. In these instances, entities will be supported through voluntary measures and assistance to achieve maturity uplift.

While this requirement will only apply to systems of national significance, it supports whole-of-critical infrastructure information sharing by building Government's threat picture to protect systems we all rely on.

# Participation in preparatory activities

Government will work with owners and operators of systems of national significance to build their cyber security capability and understanding of threats to their business through participation in 'preparatory activities', including cyber security activities and the development of playbooks.

### Cyber security activities

A key preparatory activity is participation in regular cyber security activities, in partnership with Government. These activities will build on Government's unique understanding of the threat environment, while remaining proportionate, reasonable, and sensitive to privacy. These could include: independent assessments by third-party providers; light-touch vulnerability scanning and assessment to identify vulnerabilities at the perimeter of critical networks; and Government-critical infrastructure collaboration to detect and isolate threats that have evaded existing security solutions. The benefit to owners and operators of systems of national significance and Government will be a better understanding of potential security blind spots, in turn reducing the likelihood of an incident occurring.

### Playbook

Another key activity is co-development of a playbook of response plans for a range of scenarios. This will provide owners and operators of systems of national significance with important information on 'what to do' and 'who to call' to keep their business (and customers) safe when facing a cyber attack.

Development of these playbooks will require partnership between Government and individual entities to ensure arrangements are tailored to each entity's needs and can be activated on a 24/7 basis. This will provide certainty to owners and operators of systems of national significance by outlining roles and responsibilities in the event of a significant incident, especially when a cyber attack is beyond their capability.

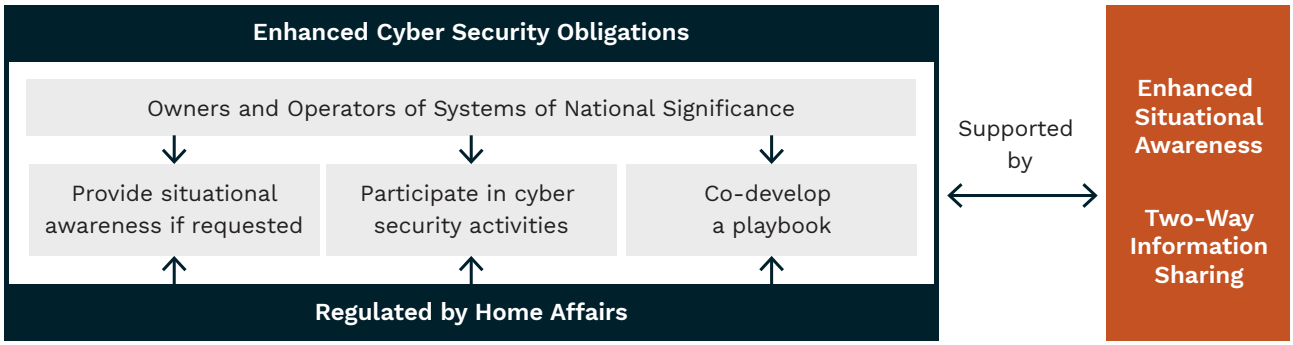



**Figure 4:** Enhanced Cyber Security Obligations – proposed initiatives

## Call for views

**22.** Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?

**23.** What information would you like to see shared with critical infrastructure by Government? What benefits would you expect from greater sharing?

**24.** What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?

**25.** What methods should be involved to identify vulnerabilities at the perimeter of critical networks?

**26.** What are the barriers to owners and operators acting on information alerts from Government?

**27.** What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?

**28.** What safeguards or assurances would you expect to see for information provided to Government?

# Initiative 3: Cyber assistance for entities

Ideally cyber incidents will be thwarted by risk management, preparatory activities and enhanced situational awareness. However, this framework would be incomplete without considering and preparing what would need to be done to protect Australia's critical infrastructure when facing a significant threat.

The third element of the framework applies Australia's strengthened situational awareness and enhanced maturity to protect all critical infrastructure and systems of national significance from cyber attacks. This recognises Government's unique understanding of Australia's threat environment and the interdependencies within critical infrastructure sectors, position it to best determine appropriate preventative actions and resource allocation in a crisis.

## Establish the capability to disrupt and respond to threats

By having a more sophisticated understanding of the threat environment, we will have a stronger foundation to identify threats and coordinate efforts to actively protect critical infrastructure. In most circumstances, Government will rely on critical infrastructure entities to take proactive steps on the basis of threat alerts and security notices, however, there may be scenarios that require Government involvement.

This model facilitates Government-critical infrastructure collaboration to protect from and mitigate the effects of cyber attacks. This benefits entities by ensuring Government capabilities are appropriately directed to protecting Australia's critical infrastructure, and by providing immunities to entities to conduct mitigations that may otherwise open them up to a civil suit.

### Entity action: Significant impacts on Australia's economy, security or sovereignty

Critical infrastructure entities may face situations where there is an **imminent cyber threat or incident** that could significantly impact Australia's economy, security or sovereignty, and the threat is within their capacity to address. In these cases, we propose that Government be able to provide reasonable, proportionate and time-sensitive **directions** to entities to ensure action is taken to minimise its impact. Entities may also be able to request that Government make such a direction, providing them with the legal authority to conduct any necessary action.

Entities must be empowered to take necessary, preventative and mitigating action against significant threats. Government recognises that entities require appropriate immunities to ensure they are not limited by concerns of legal redress for simply protecting their business and the community.

Critical infrastructure entities will only be directed to take protective or mitigating actions reasonably within their capability to address. Under no circumstances will entities be directed or authorised to take actions against the perpetrator (including 'hack backs').

### Government action: An emergency threatening Australia's economy, security or sovereignty

There may be even more limited circumstances where Government identifies an **immediate and serious cyber threat** to Australia's economy, security or sovereignty (including threat to life). In these situations, it may be appropriate for Government to declare an emergency. Further, it may also be appropriate for an alerting system at the national level, similar to the current National Terrorism Threat Advisory System, particularly for a cyber-related attack or incident.

In an emergency, we see a role for Government to use its enhanced threat picture and unique capabilities to take **direct action** to protect a critical infrastructure entity or system in the national interest. These powers would be exercised with appropriate immunities and limited by robust checks and balances. The primary purpose of these powers would be to allow Government to assist entities take technical action to defend and protect their networks and systems, and provide advice on mitigating damage, restoring services and remediation.

In determining whether an incident would constitute an emergency, the following factors will be considered:

- the potential consequence to Australia's economy, security or sovereignty;
- the extent to which the incident would spread across jurisdictions; and
- the imminence of the threat (noting it may be in progress).

It is anticipated the Government assistance element of the framework will be primarily discharged on a voluntary basis, as entities will also want to restore functions expeditiously. However, there may be cases where entities are unwilling to work with Government to restore systems in a timely manner. Government needs to have a clear and unambiguous legal basis on which to act in the national interest and maintain continuity of any dependent essential services.

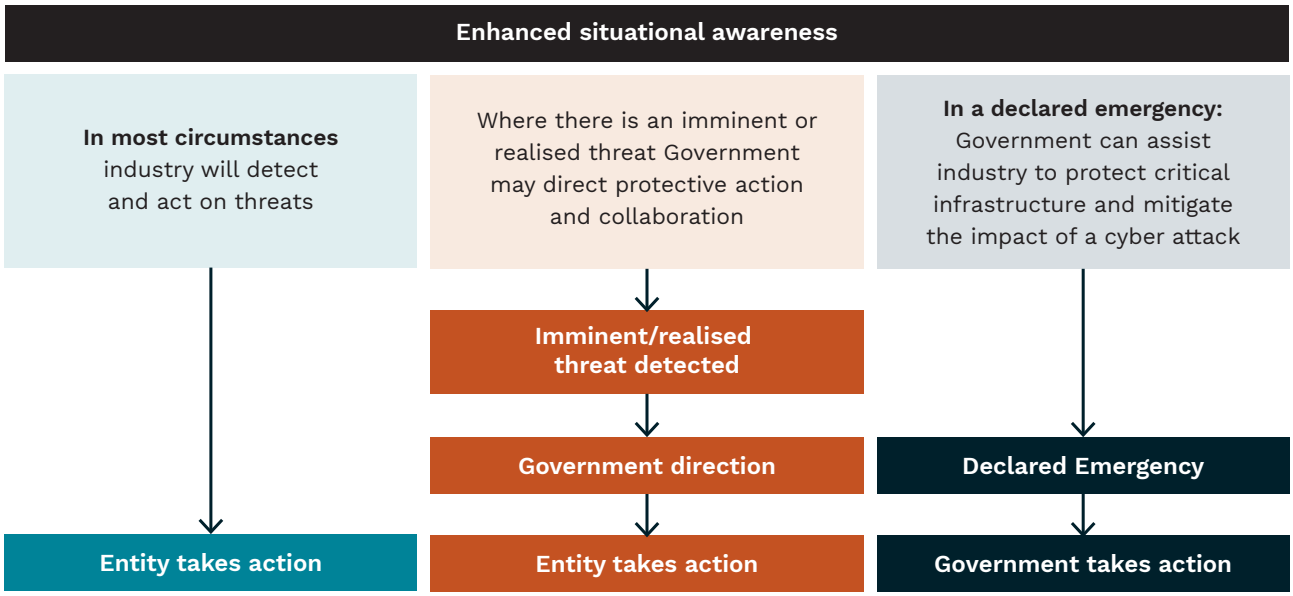



**Figure 5:** Response Model – proposed responsibilities

# Call for views

**29.** In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?

**30.** Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?

**31.** Who should oversee the Government's use of these powers?

**32.** If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?

**33.** What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?

**34.** What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?

**35.** What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?

**36.** Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?

# Call for submissions

Closing date for submissions: 5:00pm AEDT on 16 September 2020.

Submissions on this Consultation Paper are welcome from all stakeholders including critical infrastructure entities, government, academia, and members of the general public, but particularly those who will likely be covered by the new framework.

We welcome written submissions in response to any or all of the consultation questions listed in this Consultation Paper. Please provide your submissions through the **Submissions Form,** and any questions relating to the submission process to: ci.reforms@homeaffairs.gov.au.

Submissions will be made public unless you specifically request that the submission be kept confidential. The Department of Home Affairs is subject to the *Freedom of Information Act 1982* and may be required to disclose submissions in response to requests made under that Act.

The *Privacy Act 1988* establishes certain principles regarding the collection, use and disclosure of information about individuals. Any personal information respondents provide to the Department through submissions will be used for purposes related to the consideration of issues raised in this Consultation Paper, in accordance with the *Privacy Act*. If the Department makes a submission, or part of a submission, publicly available, the name of the respondent will be included. Respondents should clearly indicate in their submissions if they do not wish their name to be included in any publication relating to this consultation that the Department may publish.

## Next steps

The Government intends to consult with stakeholders during and after receiving submissions. This will also allow us to assess the impact of proposed reforms and refine the development of the enhanced framework.

Prompt action is required to ensure Australia is in a strong position to address all threats to our critical infrastructure. Legislative amendments to the Act will be developed, informed by cross-sectoral consultation on the reforms. Following introduction to Parliament, Government, and owners and operators of critical infrastructure will have the opportunity to co-design sector-specific security obligations.

# Call for views

1. Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?
2. Do you think current definition of Critical Infrastructure is still fit for purpose?
3. Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?
4. What are the common threats you routinely prepare for and those you have faced/ experienced as a business?
5. How should criticality be assessed to ensure the most important entities are covered by the framework?
6. Which entities would you expect to be owners and operators of systems of national significance?
7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?
8. What might this new TISN model look like, and what entities should be included?
9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?
10. Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?
11. Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?
12. Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?
13. What costs would organisations take on to meet these new obligations?
14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?
15. Would the proposed regulatory model avoid duplication with existing oversight requirements?
16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?
17. Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?
18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?

# Call for views

19. How can Government better support critical infrastructure in managing their security risks?
20. In the AusCheck scheme potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?
21. Do you have any other comments you would like to make regarding the PSO?
22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?
23. What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?
24. What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?
25. What methods should be involved to identify vulnerabilities at the perimeter of critical networks?
26. What are the barriers to owners and operators acting on information alerts from Government?
27. What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?
28. What safeguards or assurances would you expect to see for information provided to Government?
29. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?
30. Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?
31. Who should oversee the Government's use of these powers?
32. If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?
33. What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?
34. What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?
35. What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?
36. Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?

Australian Government

Department of Home Affairs

CRITICAL
INFRASTRUCTURE
CENTRE