Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Critical Infrastructure Resilience Strategy

February 2023

Contents

Vision

To uplift the security and resilience of Australia's critical infrastructure in the face of all hazards and advance our national security, economy and social prosperity. This will be achieved by strengthening Australia's critical infrastructure through an enhanced regulatory framework and strong collaboration across the critical infrastructure community (Figure 1).

Purpose

The *2023 Critical Infrastructure Resilience Strategy* provides a framework for how industry, state and territory governments, and the Australian Government will work together to mature the security and resilience of critical infrastructure, and to anticipate, prevent, prepare for, respond to and recover from all-hazards. This Strategy builds upon the *2015 Critical Infrastructure Resilience Strategy.*

Objectives

The *Critical Infrastructure Resilience Strategy* (the Strategy) has been developed to:

1. Support critical infrastructure owners and operators to effectively manage risks to the continuity of their operations through mature risk based and resilience approaches.
2. Deliver initiatives through strong industry–government partnerships.
3. Support critical infrastructure owners and operators to strengthen their security and resilience through regulatory frameworks, tools and improved collaboration.

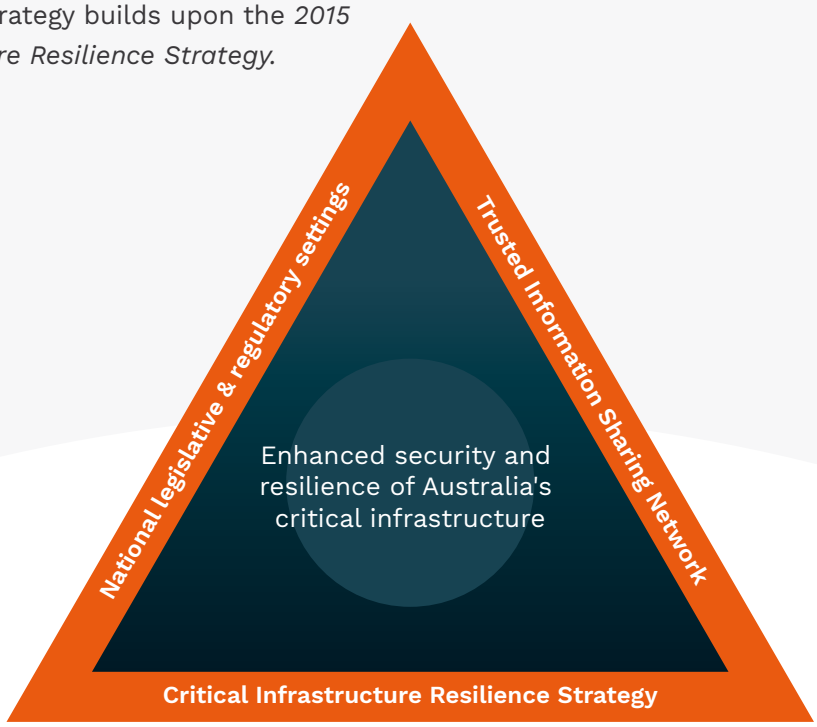


Figure 1. Complementary national initiatives

Figure 1 demonstrates the interconnectivity between the Strategy, regulatory settings provided by governments, and strong industry–government partnerships enabled through the Trusted Information Sharing Network (TISN). These initiatives must work collectively to uplift the security and resilience of Australia's critical infrastructure.

Importance of critical infrastructure

All Australians rely on critical infrastructure to deliver the essential services that underpin our economy, security and sovereignty, and support our way of life.

Critical infrastructure is defined as:

> *those physical facilities, systems, assets, supply chains, information technologies and communication networks which, if destroyed, degraded, compromised or rendered unavailable for an extended period, would **significantly** impact the social or economic wellbeing of Australia as a nation or its states or territories, or affect Australia's ability to conduct national defence and ensure national security.*

Significant impacts include events or incidents that put public safety and confidence at risk, threaten our economic and national security, harm our international competitiveness, and/or impede the continuity of government and/or industry and their ability to deliver essential services.

This Strategy, and the objectives it seeks to achieve, covers Australia's critical infrastructure priorities and outlook over 2023-28. However, the Strategy may be updated should Australia's circumstances materially change, or there is a credible development in the threat environment which would require a proactive response.

The *Critical Infrastructure Resilience Plan* (the Plan), which accompanies this Strategy, sets out how the Strategy's objectives will be delivered. The Plan adopts a multi-year outlook, and allows for the monitoring and evaluation of activities.

The Plan will be updated by the Department of Home Affairs in consultation with the Critical Infrastructure Advisory Council on an as-needed basis.

An evolving operating environment

The context in which Australia's critical infrastructure operates has materially changed since the *2015 Critical Infrastructure Resilience Strategy* Policy Statement and Plan were launched.

Across the world, cybercrime targeting essential services – such as the health care, food distribution and energy sectors – has demonstrated the vulnerability of critical infrastructure. The Australian Cyber Security Centre (ACSC) observe that the cyber threat to Australia's critical infrastructure is an enduring concern, and that State actors and cybercriminals view critical infrastructure as an attractive target.

Similarly, the Australian Security Intelligence Organisation (ASIO) noted that the increasingly interconnected nature of Australia's critical infrastructure exposes vulnerabilities that, if targeted, could result in significant consequences for our economy, security and sovereignty. ASIO remains concerned about the potential for Australia's adversaries to pre-position malicious code in critical infrastructure, particularly in areas such as telecommunications and energy.

The pandemic and various natural hazards demonstrate the significant impact such disruptions can have on communities and the Australian way of life. Geopolitical developments underscore the reliance of critical infrastructure on its supply networks, including upstream supply chain flows, production, and downstream distribution networks.

Disruptions to critical infrastructure systems can result from other types of natural and human-made hazards and threats, such as major weather events or human error.

Such disruptions can create a chain of cascading consequences with profound effects on societies and communities, and interconnected infrastructure systems.

The impacts of disasters can be long term, complex and have a cascading bearing on daily life and the social and economic wellbeing of communities. These events highlight the nation's reliance on our critical infrastructure, its interconnected systems, the challenges in maintaining it, and in some instances the fragility of systems such as supply chains and the workforce.

For example, a prolonged and widespread failure in the energy sector would have a nationally significant effect, such as:

impacts to water supply and sanitation, and in turn public health

reduced services or shutdown of the banking, finance and retail sectors

instability in the supply of food and groceries

disruptions to transport and telecommunications networks

impacts to delivery of health services and medical supplies

impacts to government and its services.

Critical infrastructure owners and operators provide essential services on which the community depend. Our communities will experience more compounding events as a result of natural hazards, and will continue to play a key role in responding to these risks. Therefore, it is important for critical infrastructure, and the communities it serves, to adapt to this changing landscape and to deliver outcomes for them through regulatory settings provided by governments, and strong industry-government partnerships.

Future security and resilience initiatives need to consider how the context of our operating environment will be subject to constant change. We need to consider the impact of:

- susceptibility to a wider range of hazards, from physical and natural (including extreme weather events on unprecedented scale, frequency and intensity as a result of climate change), supply chain and personnel, to cyber and information security.
- technological advances and increased connectivity. More systems and services are being connected to the internet and to each other, creating economic efficiencies but also increasing the likelihood and impact of disruptions.
- an increasingly volatile geopolitical environment, and susceptibility of critical infrastructure to attack by nation states, state-sponsored actors, issue motivated groups, or extremist groups, seeking to advance their own interests.

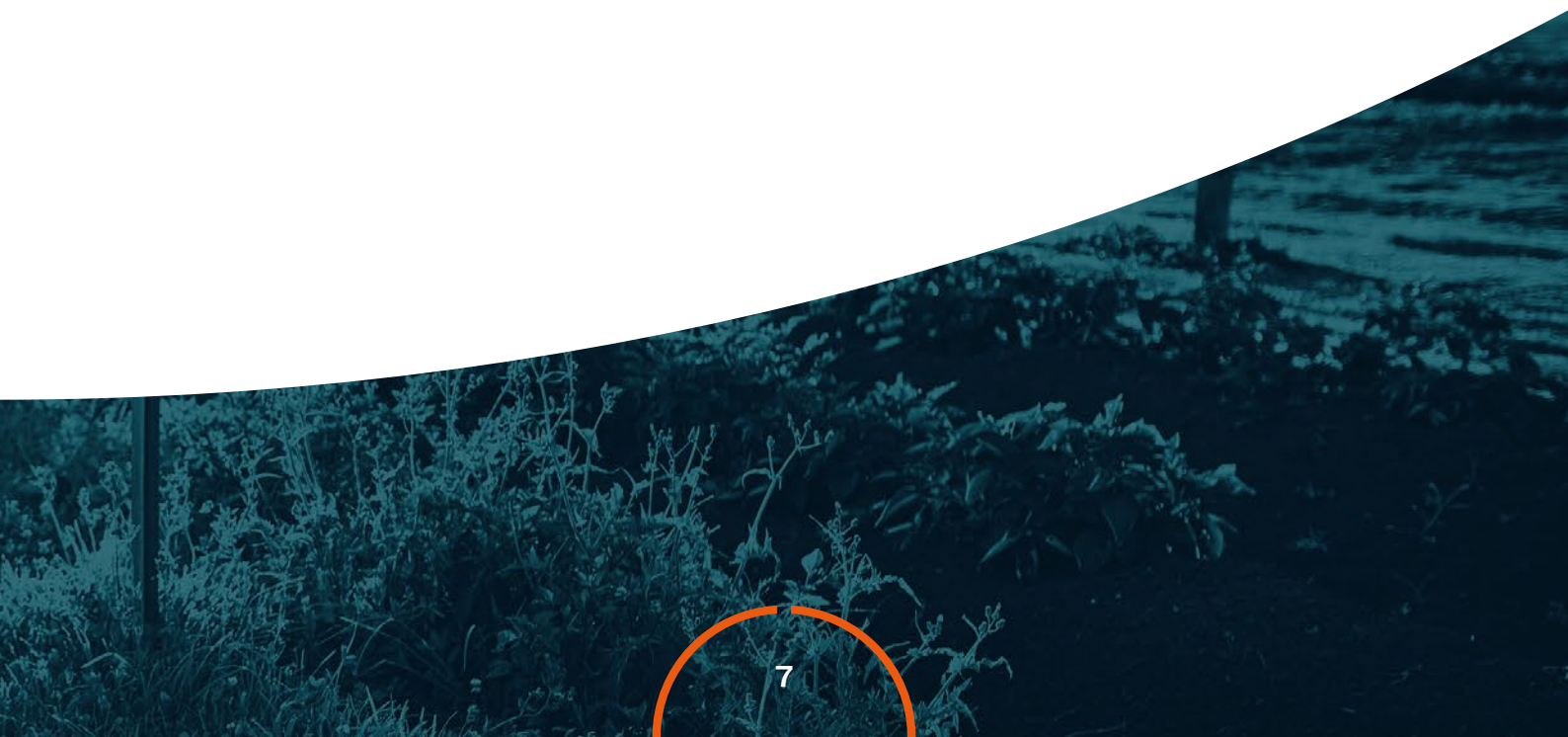
Resilience and risk

The concept of *organisational resilience* refers to a business' ability to adapt to an evolving global market, to respond to short-term shocks – whether natural hazards or significant changes in market dynamics – and to shape itself to respond to long-term challenges.

For the purpose of this Strategy, *critical infrastructure resilience* refers to those aspects of organisational resilience that focus on measures to uplift the security and resilience of critical infrastructure owners, operators and supply-network stakeholders as a collective and across the whole economy.

These measures include resilience support provided through the Trusted Information Sharing Network, initiatives under the *Critical Infrastructure Resilience Plan* and initiatives ensuring well-informed and robust risk management processes that take account of:

- material risks that have a substantial impact on the availability, reliability and integrity or confidentiality of government and/or a critical infrastructure assets and the services they deliver
- cyber and information security hazards
- personnel hazards
- supply chain hazards
- physical and natural hazards.



Regulatory settings

Australia's critical infrastructure is regulated through Commonwealth, and state and territory legislation. These legislative and regulatory settings are augmented by industry codes of practice, as well as emergency management arrangements. For example, in the event of emergencies, the Australian Government Crisis Management Framework (AGCMF), the National Coordination Mechanism (NCM) and long-standing state and territory emergency and crisis management arrangements may be stood-up.

Australia's regulatory settings must keep ahead of the evolving all-hazards environment to support national security and resilience.

The Commonwealth *Security Legislation Amendment (Critical Infrastructure) Act 2021* (SLACI Act) amended the *Security of Critical Infrastructure Act 2018*, requiring regulated owners and operators of Australia's critical infrastructure to take steps to better protect infrastructure.

The SLACI Act broadened the range of risks to be managed and the number of sectors captured as critical infrastructure to include:

Communications

Data storage or processing

Financial services and markets

Water and sewerage

Energy

Health care and medical

Higher education and research

Food and grocery

Transport

Space technology

Defence industry

It established mandatory cyber incident reporting, with responsible entities for critical infrastructure assets required to report certain cyber security incidents to the ACSC. It also expanded the number of asset classes that need to provide owner and operator information to the Register of Critical Infrastructure Assets.

Importantly the SLACI Act granted the Australian Government the ability to provide government assistance to state and territory government and critical infrastructure entities in response to serious cyber-attacks on Australian systems.

The *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (SLACIP Act) further amended the *Security of Critical Infrastructure Act 2018* to enact a framework for risk management programs, declarations of systems of national significance, and enhanced cyber security obligations. These elements will improve the preparedness of critical infrastructure entities to manage and mitigate the range of hazards that could otherwise have a serious impact on the delivery of their essential service.

The reforms reflect the importance the Australian Government places on assisting our critical infrastructure entities to tackle the evolving threats that have the potential to significantly impact the delivery of Australia's essential services.

Non-regulatory settings

The Trusted Information Sharing Network (TISN) is industry and all levels of government's primary way of engaging to enhance the security and resilience of critical infrastructure. The TISN brings together critical infrastructure owners and operators, supply chain entities, peak bodies and all levels of government, and is focused on key critical infrastructure sectors in Australia (Figure 2). It is a trusted, non-competitive environment for the critical infrastructure community to better plan, prepare, respond and recover in the face of all-hazards.

The TISN was first established by the Australian Government in April 2003 in the post-9/11 environment, with an initial focus on counter terrorism mainly through bilateral engagement.

The TISN's focus has evolved to meet the contemporary challenges being faced across Australia, including the whole-of-economy impacts of the COVID-19 pandemic and the significant disruptions caused by natural events such as the 2019–20 bushfires and the 2022 floods. The TISN has become a more sophisticated network, focusing on an all-hazards and all-sectors approach, providing flexible collaboration and multilateral engagement for members, within a new regulatory context.

TISN members collaborate to strengthen the resilience of their organisations, sectors, and the overall network, and to deliver the vision of the Strategy. The forum provides the opportunity for members to:

- collaborate, learn, share information, research and innovate
- create ongoing trusted partnerships and engage flexibly with industry, all levels of government and the wider critical infrastructure community
- coordinate industry-government engagement and approaches to enhance resilience
- build maturity and engagement across and within organisations and sectors of the TISN
- facilitate understanding of, and compliance with regulatory frameworks
- discuss asset vulnerabilities and implement mitigation strategies to ensure resilience for continued operation.

TISN Sector Groups enable critical infrastructure owners, operators and regulators from the same sector to share information on threats and vulnerabilities, and collaborate on appropriate measures to manage risk and increase resilience.

The TISN does not have an operational role; however it supports national prevention, preparedness, response and recovery activities of members by connecting stakeholders. It does not replace existing response mechanisms such as the AGCMF, state emergency management capabilities and arrangements, commercial contractual and other existing regulatory requirements and arrangements.

The Department of Home Affairs is responsible for the TISN, with other Commonwealth government agencies playing an active role by contributing expertise and running Secretariat functions for certain sector groups. Activities to strengthen the TISN are detailed in the Critical Infrastructure Resilience Plan.

Where are we taking the TISN?

TISN Trusted Information Sharing Network

The TISN is evolving as a flexible network that enables critical infrastructure community members to collaborate more effectively between sectors on cross-sector and cross network issues. Due to its flexible nature, the TISN may see the emergence of new sector and segment groups. The asset classes captured by the *Security of Critical Infrastructure Act 2018* are an important part of the enhanced TISN and as such are clearly identified within relevant TISN sector groups, to enable engagement on regulatory reform activities.

TISN members have an increasing ability to choose how they engage, to focus on areas of interest and more easily collaborate with other members who are addressing similar issues, better enabling them to increase their organisation's resilience capability. This will occur within the framework of governance arrangements that are set within the context of each sector and documented within the sector groups' Terms of Reference.

Figure 2: Critical infrastructure engagement

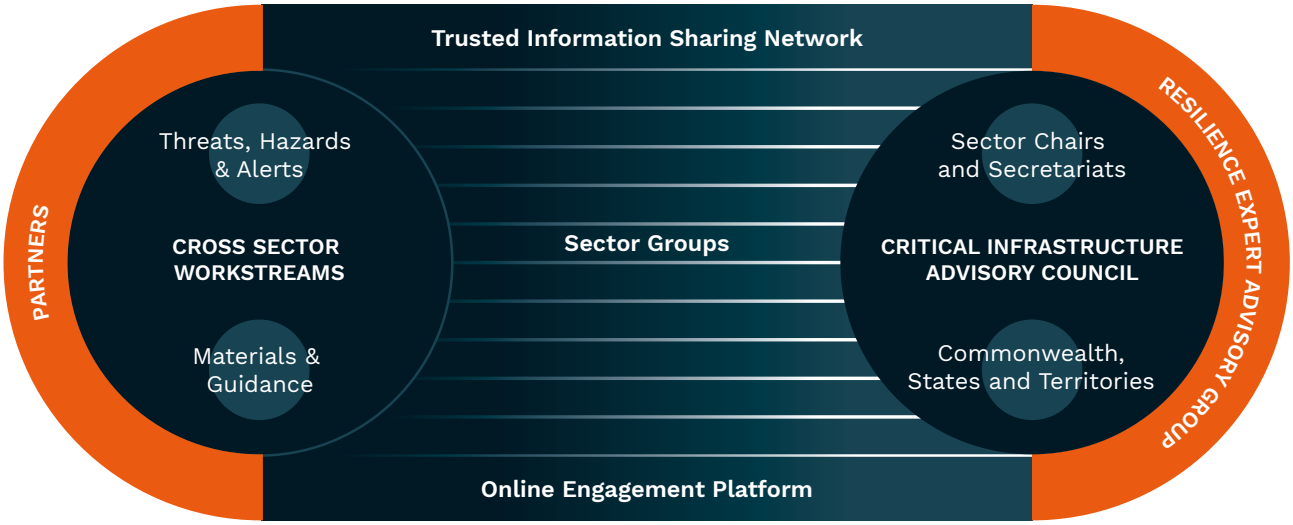


Figure 2 demonstrates the national coordination arrangements for critical infrastructure engagement and uplift. It reflects the organisational structure of the Critical Infrastructure Advisory Council (CIAC), and its sector, cross-sectoral and advisory groups. Entities such as CIAC play a key role in ensuring the security and resilience of Australia's critical infrastructure by providing strategic direction and priorities for the TISN.

Stakeholder responsibilities

The Australian Government, state and territory governments, and industry collectively contribute to Australian critical infrastructure security and resilience, and ensure the Strategy's objectives are realised. The roles for each entity are outlined below.

STAKEHOLDER	RESPONSIBILITIES	CROSS-CUTTING RESPONSIBILITIES
Australian Government	• Develop and align legislation and regulations that advance national settings to strengthen critical infrastructure resilience • Ensure arrangements are in place for information sharing (such as threat information) and collaboration on risk and resilience initiatives	• Develop best practice guidance to enhance security and resilience of critical infrastructure • Work collaboratively to enhance the resilience of critical infrastructure and achieve the objectives of the Strategy and TISN • Engage in information sharing and exchange to promote mutual understanding and trust across industry, local, state, territory and Australian governments • Implement lessons learned strategies to limit the impact of hazards and threats • Understand cross-sector dependencies and collectively work to address sectoral vulnerabilities and resilience gaps • Collaborate nationally to design and implement regulatory frameworks • Undertake prevention, preparedness, response and recovery activities in line with the risk management program obligations for all hazards, and utilise the TISN and Australian Government Crisis Management Framework when required
State and territory governments	• Develop legislation, regulations and collaborative arrangements that advance jurisdictional settings to strengthen critical infrastructure resilience • Support jurisdiction-owned/operated critical infrastructure in managing and minimising risks to continuity in the event of any disruption	
Industry	• Manage risks and enhance resilience for their owned/operated critical infrastructure • Participate in risk identification, assessment, prevention, mitigation, preparedness, response and recovery activities	

The effort to uplift national critical infrastructure security and resilience is coordinated, harnessed and realised through the TISN framework. The TISN comprises the Critical Infrastructure Advisory Council, its sectors and advisory groups. This structure is described below.

STAKEHOLDER	RESPONSIBILITIES
Critical Infrastructure Advisory Council (CIAC)	Provide leadership and strategic direction for the TISN on matters of critical infrastructure resilience, including overseeing the implementation of the Critical Infrastructure Resilience Strategy and the Critical Infrastructure Resilience Plan, advocating and engaging across government, and monitoring the work of Sector and Advisory groups
TISN Sector Groups	Collaborate and champion critical infrastructure resilience security and resilience initiatives, and represent the interests of owners and operators of critical infrastructure to government
Advisory Group*	Provide advice and support the development of tools, guidance material, education and outreach programs to support owners and operators of critical infrastructure to uplift security and resilience Provide support and guidance to CIAC and TISN on emerging and future resilience trends and issues **The Department of Home Affairs primarily engages with a resilience focused advisory group, the Resilience Expert Advisory Group. Additional groups may emerge following future regulatory reforms.*

Critical Infrastructure Resilience Plan

The *2023 Critical Infrastructure Resilience Strategy* is accompanied by a *2023 Critical Infrastructure Resilience Plan* (the Plan).

The Plan outlines national activities that the Cyber and Infrastructure Security Centre (CISC) and the Australian critical infrastructure community will pursue to realise the objectives outlined in this Strategy.

The Plan is a living document that will be considered annually in partnership with Critical Infrastructure Advisory Council (CIAC) and TISN Sector groups, and updated where circumstances necessitate.

Australian Government

Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE