Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Critical Infrastructure Resilience Plan

February 2023

Critical Infrastructure Resilience Plan 2023

The *Critical Infrastructure Resilience Strategy 2023* (the Strategy) provides the high-level policy direction that underpins Australia's approach to critical infrastructure resilience. The Strategy identifies three overarching objectives to uplift Australia's security and resilience:

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 frameworks, tools and improved collaboration.**

This Critical Infrastructure Resilience Plan 2023 (the Plan) outlines national activities that the Cyber and Infrastructure Security Centre (CISC) and the Australian critical infrastructure community will pursue to realise these objectives.

It 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.

The CISC is responsible for supporting the delivery of all activities in partnership and consultation with the Critical Infrastructure Advisory Council, the Resilience Expert Advisory Group and TISN members. The CISC, in partnership with these stakeholders, will evaluate the deliverables under this Plan annually.

REF	ACTIVITY	DELIVERABLES	TIMEFRAME	OBJECTIVES
1	**Extend and enhance the Trusted Information Sharing Network (TISN)**	Roll out the TISN collaborative platform to all existing sector groups to streamline engagement and access to materials and ease secretariat burden.	2023-2024	2, 3
		Extend the TISN to include: • expansion of sectors and introduction of sector segmentation to reflect the whole of the economy, and to include groups captured by the legislation • expansion of TISN membership with: – functional representatives from organisations – more industry organisations and peak bodies – relevant state and territory representatives, from both First Minister departments and line agencies that align with each sector group – groups captured by the legislation • introduction of cross-sector workstreams • an online platform to streamline engagement • updated governance to support network changes	2023-2024	2, 3
		Establish cross-sector workstreams which enable TISN members to engage on identified threats and hazards that may impact one or more sectors, with clear industry and government leads/experts, in policy, operational and intelligence areas, who shape, guide and contribute to engagement within each workstream. Enable all TISN members – industry and government – to collaborate in this area to develop a stronger security and resilience approach to the identified threats and hazards.	2023-2024	2, 3
		Extend the TISN to include new advisory groups when required.	Ongoing	2, 3
		Implement and mature membership and broaden the base of expertise and representation by including a new membership category of non-sector specific members called partners, who may be industry experts, academia, supply chain entities or peak bodies.	2023-2024	2, 3

REF	ACTIVITY	DELIVERABLES	TIMEFRAME	OBJECTIVES
		Develop and implement TISN governance arrangements (namely Terms of Reference and procedures) and ensure they are reviewed annually to ensure operations are efficient, effective and risks managed.	Annually	1, 2, 3
		TISN Sector Groups establish and drive their individual sector work plans – revised annually – and support cross-sectoral engagement, consistent with the Strategy and guidance from CIAC.	Annually	1, 2, 3
2	**Support TISN members to uplift critical infrastructure security and resilience**	Provide and promote contemporary best-practice guidance on industry resilience.	June 2023	1, 2, 3
		Examine and rebuild the resilience HealthCheck tool and refine the resilience indicators.	June 2023	1, 2, 3
		Identify, map out and document the critical infrastructure supply chain risks to inform and engage with the Sovereign Capability Manufacturing Plans, and developing strategies of the Office of Supply Chain Resilience.	Ongoing	1,2,3
		Provide useable and actionable threat information to support regulators, owners and operators to uplift security and resilience.	Ongoing	1, 2, 3
		Increase sector-level understanding of nationally significant critical infrastructure assets, supply chains and interdependencies, and strengthen collaboration on resilience practices, through the sharing of views on strategic issues, trends and hazards, so that critical infrastructure owners, operators and regulators may assess and manage risk appropriately.	Ongoing	1, 2, 3
		Provide industry-level cross-sector visualisation of dependencies and risk exposure based on input information.	Ongoing	1, 3
		Produce and distribute sector-specific risk assessments aimed at providing industry and government entities with tangible mitigation strategies to enhance their security posture, to be informed by threat information and landscape scanning from the Australian Cyber Security Centre.	Ongoing	1, 3

REF	ACTIVITY	DELIVERABLES	TIMEFRAME	OBJECTIVES
		Exchange information on good practice standards as well as during and post-event learnings with jurisdictions, industry and international partners on critical infrastructure resilience and security.	Ongoing	1, 2, 3
		Ensure industry is able to advise government on security and resilience matters, including: risks; supply chain vulnerabilities; incident management, business continuity and post-incident lessons.	Ongoing	1, 2, 3
		Establish and implement a multi-year work plan to uplift organisational and sectoral resilience.	2023-26	1, 2, 3
3	**Support critical infrastructure owners and operators to meet their regulatory obligations**	As a responsive regulator, support critical infrastructure industry participants to uplift security and resilience through educational activities.	Ongoing	1, 2, 3
		Deliver educational and guidance materials to assist critical infrastructure owners and operators in meeting their obligations under the *Security of Critical Infrastructure Act 2018*.	December 2023	2, 3
		Support national efforts to respond to the impacts on critical infrastructure from hazards, such as natural hazards and human induced threats to supply chain issues, including through an exercise management function that supports the delivery of exercises for national crisis response operations and serious cyber incidents impacting critical infrastructure assets. These exercises are conducted in partnership with Commonwealth and state and territory counterparts, and critical infrastructure asset owners and operators.	Ongoing	1, 2

Australian Government

Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE