SOCI 2019 Compliance Obligations Summary Table

Table 1. Summary of Critical Infrastructure Compliance Obligations under the SOCI Act 2018

Obligation	Explanation	Reference	Who needs to do this	Due Date
Notify data service providers	Entities must notify external data service providers if they are storing or processing business critical data. This ensures that companies that are handling sensitive data for critical infrastructure assets are aware that they may themselves also have obligations under the Act and that they treat the security of the data appropriately.	SOCI Act Subsection 12F(3)	A responsible entity for a critical infrastructure asset that has business critical data processed or stored by a third party on a commercial basis must, as soon as reasonably practicable, take reasonable steps to inform the third party that they are processing or storing business critical data of a critical infrastructure asset.	December 2021
Reporting Information	The Register of Critical Infrastructure Assets requires reporting entities, who are either direct interest holders or the responsible entity of critical infrastructure assets, to provide to Government ownership, operational, interest and control information. Responsible entities are required to provide updated information where operational information previously provided becomes incorrect or incomplete, or the reporting entity for an asset changes. These updates must be made within 30 days of the event occurring.	Part 2 of the SOCI Act: Register of Critical Infrastructure Assets Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022 Register of Critical Infrastructure Assets Guidance	Responsibility entities and a direct interest holder for asset classes defined in section 12L: • broadcasting • domain name system • data storage or processing • a critical financial market infrastructure asset that is a payment system • food and grocery • hospital • freight infrastructure • freight services • public transport • liquid fuel • energy market operator • electricity (that were not within the scope of a critical infrastructure asset prior to the SLACI Act amendments); and • gas (that were not within the scope of a critical infrastructure asset prior to the SLACI Act amendments).	If the responsible entity's asset became a critical infrastructure asset before 8 April 2022, the responsible entity is required to provide the asset's operational information by 8 October 2022. If the responsible entity's asset became a critical infrastructure asset after 8 April 2022, the responsible entity is required to provide the asset's operational information **within 6 months of the day the asset became a critical infrastructure asset.** Updates to information provided must be made **within 30 days of the event occurring.**
Mandatory cyber incident reporting	Responsible entities for critical infrastructure assets will be required to report critical and other cyber security incidents to the Australian Cyber Security Centre's online cyber incident reporting portal	Part 2B of the SOCI Act Cyber Security Incident Reporting ACSC Critical Infrastructure Uplift Program	• broadcasting • domain name system • data storage or processing • banking • superannuation • insurance • financial market infrastructure • food and grocery • hospital • education • freight infrastructure • freight services • public transport • liquid fuel • energy market operator • aviation, that is any of the following: ○ a designated airport	**8 April 2022** Grace period: 3 months **8 July 2022**

Obligation	Explanation	Reference	Who needs to do this	Due Date
			○ an Australian prescribed air service operating screened air services that depart from a designated airport, or ○ a regulated air cargo agent that is also a cargo terminal operator at a designated airport. • ports • electricity • gas; and • water.	
Adopt a written CIRMP	Adopt, maintain and comply with a written Critical Infrastructure Risk Management Program. Entities must have and comply with a Risk Management Program for their critical infrastructure assets. This will ensure responsible entities have a comprehensive understanding of the threat environment, and develop processes and procedures to effectively respond to the material risk of any hazard impacting their asset.	SOCI Act Part 2A: Risk Management Program CIRMP resources	• Broadcasting • Domain Name Systems • Data Storage or processing • Electricity • Energy Market Operator • Gas • Liquid Fuels • Payment Systems • Food and Grocery • Designated Hospitals (listed in Schedule 1 of the CIRMP Rules) • Critical Freight Infrastructure (Under the SOCI Act only intermodal facilities listed in Schedule 1 of the *Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021* are Critical Freight Infrastructure assets) • Critical Freight Services • Water	**17 February 2023**
Achieve compliance with cyber security framework identified in written CIRMP	The cyber security frameworks that can be adopted and complied with are: Australian Standard AS ISO/IEC 27001:2015, Essential Eight Maturity Model published by the Australian Signals Directorate (maturity level one), Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology of the United States of America, Cybersecurity Capability Maturity Model published by the Department of Energy of the United States of America (Maturity Indicator Level 1), or 2020 21 AESCSF Framework Core published by Australian Energy Market Operator Limited (Security Profile 1).	Guidance for Critical Infrastructure Risk Management Program	• Broadcasting • Domain Name Systems • Data Storage or processing • Electricity • Energy Market Operator • Gas • Liquid Fuels • Payment Systems • Food and Grocery • Designated Hospitals (listed in Schedule 1 of the CIRMP Rules) • Critical Freight Infrastructure (Under the SOCI Act only intermodal facilities listed in Schedule 1 of the *Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021* are Critical Freight Infrastructure assets) • Critical Freight Services • Water	**17 August 2024**
Annual Report	Entities are required to provide an annual report to the relevant Commonwealth regulator or the Secretary of the Department of Home Affairs, regarding the entity's CIRMP. Entities must submit this report within 90 days after the end of the financial year and the report must be approved by the entity's board, council, or other governing body. The report must be in the approved form and state whether the risk management program was up to date,	Guidance for Critical Infrastructure Risk Management Program	• Broadcasting • Domain Name Systems • Data Storage or processing • Electricity • Energy Market Operator • Gas • Liquid Fuels • Payment Systems • Food and Grocery • Designated Hospitals (listed in Schedule 1 of the CIRMP Rules)	The first annual report required under the CIRMP Rules is for the 2023-2024 Australian financial year. As the report must be submitted within 90 days after the end of each financial year the entity had a CIRMP in place, the first annual report must be submitted

Obligation	Explanation	Reference	Who needs to do this	Due Date
	any variations to the program, and details of how the program was effective in mitigating any relevant impacts that hazards may have had on that asset during that year. The report does not need to contain the full risk management program, but must advise the relevant Commonwealth regulator or the Secretary whether the program remains up to date.		• Critical Freight Infrastructure (Under the SOCI Act only intermodal facilities listed in Schedule 1 of the *Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021* are Critical Freight Infrastructure assets) • Critical Freight Services • Water	between 30 June 2024 and 28 September 2024.
Enhanced Cyber Security Obligations (ECSO)	The Minister for Home Affairs, after consultation with the responsible entity and others, may declare an asset to be a 'System of National Significance'. These assets are those that are most crucial to the nation, by virtue of their interdependencies across sectors and consequences of cascading disruption to other critical infrastructure assets and sectors. If declared to be a system of national significance, the responsible entity may be notified that they are subject to four additional obligations focused on cyber preparedness and resilience.	SOCI Act Part 2C: Enhanced Cyber Security Obligations (ECSO) The Enhanced Cybersecurity Obligations Framework	• System of Nation Significance	**Effective 2 April 2022**