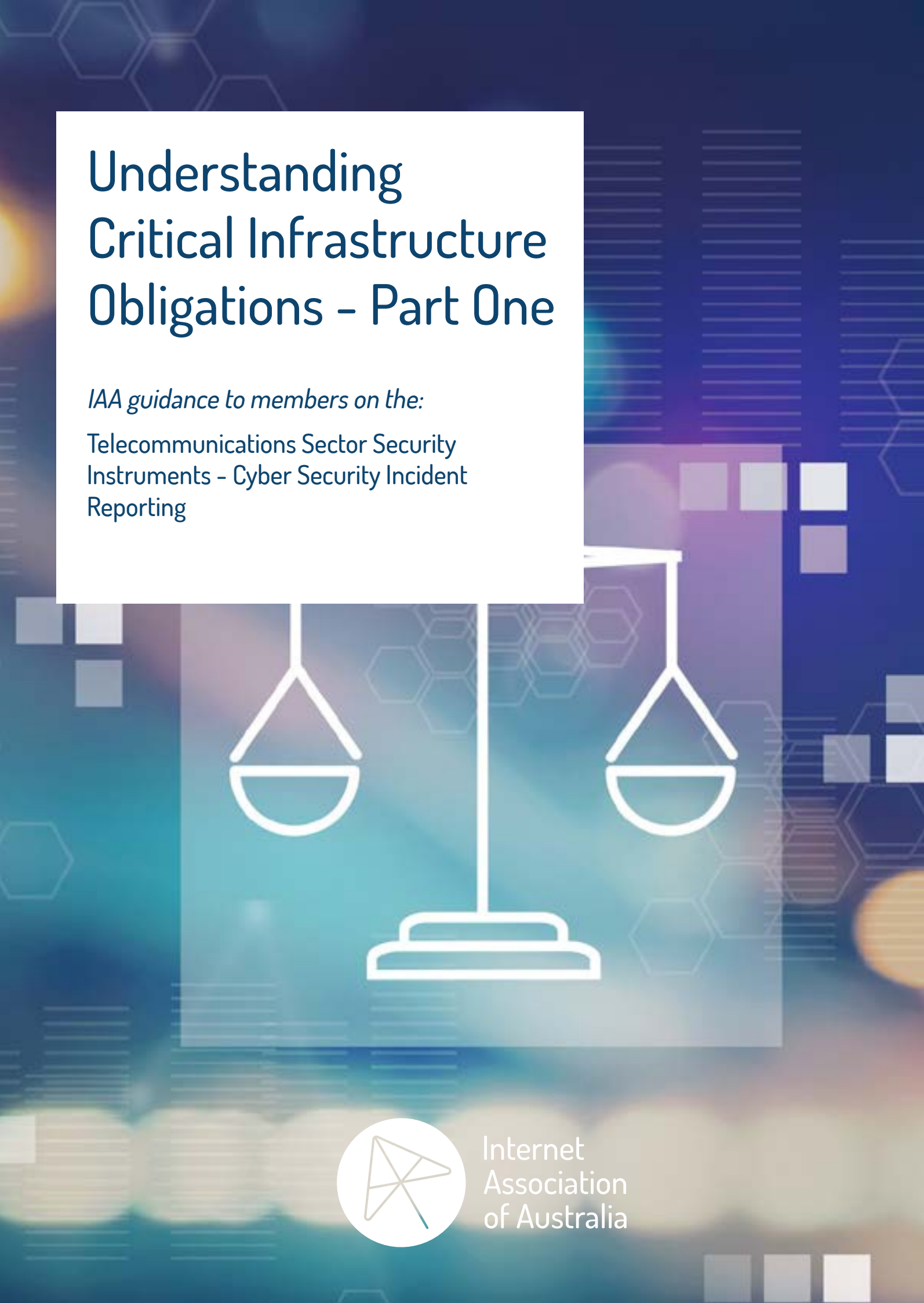
Understanding Critical Infrastructure Obligations - Part One

IAA guidance to members on the:

Telecommunications Sector Security Instruments - Cyber Security Incident Reporting



Internet Association of Australia

Contents

Title: Understanding Critical Infrastructure Obligations - Part One, IAA guidance to members
Author: Sophia Joo
Published: July 2022

Executive Summary

IAA's guide to new mandatory 'cyber security incident' reporting obligations

On 7 July 2022, the security instruments, *Telecommunications (Carrier License Conditions – Security Information) Declaration 2022* and the *Telecommunications (Carriage Service Provider – Security Information) Determination 2022* ('Telco Security Instruments') came into force, activating new rules for carriers and carriage service providers.

In response to growing risks to the security and resilience of Australia's critical infrastructure, the *Security of Critical Infrastructure Act 2018* (SOCI Act) was amended in Dec 2021, introducing new obligations for a number of sectors, including the telecommunications sector.

In order to avoid regulatory duplication, some of the obligations will be introduced under the *Telecommunications Act 1997* (Tel Act) for the telco sector, including mandatory reporting of cyber security incidents and lodging an asset register. The mandatory reporting obligations commenced 7 July 2022, and the asset register obligation will commence from 7 October.

This paper seeks to guide members in understanding and complying with the mandatory cyber security incident reporting obligations, under which significant and relevant cyber security incidents now need to be reported to the ACSC. The requirements concerning the asset register will be covered separately in Part Two.

Glossary & Key Terms

Approved Form: see 'incident reporting webform' on page 9

ACSC: Australian Cyber Security Centre

Leads the Australian Government's efforts to improve cyber security. The ACSC is based within the ASD

Incident reporting is made to the ACSC

ASD: Australian Signals Directorate

Australia's foreign signals intelligence and security agency

Asset: a tangible asset that is owned or operated by a carrier/CSP and used to supply a carriage service. Includes a component of a telecommunications network, a telecommunications network itself, a facility, computers, computer devices, computer programs, and computer data

It excludes equipment on customer premises

CISC: Cyber and Infrastructure Security Centre

The CISC is based within the Department of Home Affairs and drives the critical infrastructure regime under the Department

Critical infrastructure assets will be reported to the CISC

Cyber Security Incident: one or more events that involve:

- unauthorised access to, modification, or impairment of a computer data or computer program; or
- unauthorised impairment of the availability, reliability, security, or operation of a computer, computer data or computer program; or
- unauthorised impairment of an asset operated

Glossary & Key Terms

Essential Goods and Services: the instruments intend to only capture goods and services that are critical to the health, safety or good order of the Australian community

Relevant Impact: includes direct or indirect impact of cyber security incident on the availability, integrity, reliability or confidentiality of an asset or data or information stored in an asset

For example, services are not disrupted but workarounds have to be put in place to ensure accessibility of services

Significant Impact: the incident has materially disrupted the availability of an asset that is used for the provision of essential goods and services. It includes direct or indirect impact of the cyber security incident on the availability of the asset.

For example, an authentication system is breached and a CSP is unable to provide internet services and likely to result in outages for customers

Telco Security Instruments: refers to the two new instruments

- *Telecommunications (Carrier License Conditions – Security Information) Declaration 2022*
- *Telecommunications (Carriage Service Provider – Security Information) Determination 2022*

The instruments mirror the same obligations for carriers and CSPs and any reference to specific provisions in this guide will be referring to both instruments unless otherwise specified

Unauthorised: where the person who is causing the access, modification, or impairment is not entitled to do so

New Rules

Who do they apply to?

Carriers:

- applies to all entities/persons who hold a carrier licence on, or have been granted a carrier licence after, 7 July 2022
  - *Telecommunications (Carrier Licence Conditions – Security Information) Declaration 2022* – s 10

Carriage service providers:

- applies to all carriage service providers who supply a carriage service that enables end-users to access internet
- applies to carriage service intermediaries who arrange for the supply of services that enable end-uders to access internet
- 'end-users' may also be business users, not simply home services
  - *Telecommunications (Carriage Service Provider – Security Information) Determination 2022* – s 10

New Rules

What are the new rules?

Mandatory Reporting of Cyber Security Incidents

Notification of Critical Cyber Security Incidents

- a carrier/CSP must give the ACSC a report about a cyber security incident that has had, or is having, a **significant impact** on any of its assets as soon as reasonably practicable or **no later than 12 hours** after becoming aware of the incident
- report may be given orally or in writing in the approved form
- if report is given orally, the carrier/CSP must make a written record of the report in the approved form to the ACSC within 84 hours of initial report
- Cf. s 11

Notification of Other Cyber Security Incidents

- a carrier/CSP must give the ACSC a report about a cyber security incident that has had, or is having, a **relevant impact** on its asset as soon as reasonably practicable or **no later than 72 hours** after becoming aware of the incident
- report may be given orally or in writing in the approved form
- if report is given orally, the carrier/CSP must make a written record of the report to the ACSC within 48 hours of initial report
- Cf. s 12

What This Means For You

Changes to policy often means changes for you and your business.

Develop potentially new procedures and systems to assist in identifying disruptions to assets that are “cyber security incidents”

Employee training in:

- identifying cyber security incidents
- the difference between “critical” and “other” cyber security incidents
- correctly reporting cyber security incidents to the ACSC

Ensure your assets and systems are secured and protected from cyber security threats

Helpful Contacts & Material

Regulation can be difficult to understand, so talk to people and access information for further guidance!

Internet Association of Australia Ltd
02 9037 6404
policy@internet.asn.au
www.internet.asn.au

CISC:
1300 27 25 24
enquiries@CISC.gov.au
https://www.cisc.gov.au/

ACSC:
Urgent Oral Reports: 1300 292 371
Incident Reporting Webform
Guidance Material
Fact Sheet
www.cyber.gov.au

DITRDC
telsecurityreview@communications.gov.au
Carrier Licence Declaration
CSP Determination
Explanatory Statement