DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY SPOKEN QUESTION ON NOTICE

Senate Economics References Committee

22 August 2023

QoN Number: 3

Subject: Enforcement mechanisms in relation to critical infrastructure assets, including powers, provisions and compliance

Asked by: Andrew Bragg

Question:

CHAIR: I just want to circle back on my initial question. Is anything you can provide us on notice about the enforcement mechanism you have in relation to the critical infrastructure assets that have been designated and how you would go about bringing an action?
Mr Hansford: Certainly. I can outline to you both the penalties and indeed the criminal offences that apply for the breach of the use of a part 3A power. I can provide you with those, and then, more generally, I can provide information about the general provisions in the Regulatory Powers (Standards Provisions) Act which would apply to the implementation and the exercise of enforcement and compliance of the Security of Critical Infrastructure Act.
CHAIR: That would be very helpful.

Answer:

Penalties under the *SOCI Act*

The *Security of Critical Infrastructure (SOCI) Act* includes a number of civil penalty provisions for non-compliance with different obligations, including the examples set out in the following table.

Provision	**Obligation civil penalty applies to**	**Maximum penalty**
s 30AC	Responsible entity must adopt and maintain a critical infrastructure risk management program that applies to the entity	200 penalty units
s 30AG	Responsible entity must submit an annual report about its critical infrastructure risk management program within 90 days after the end of the financial year	150 penalty units

Provision	Obligation civil penalty applies to	Maximum penalty
s 30BC(1)	Responsible entity must give the relevant Commonwealth body a report about a critical cyber security incident as soon as practicable, and in any event within 12 hours of becoming aware of the incident	50 penalty units
s 30CD	Responsible entity for a System of National Significance to which the statutory incident response planning obligation applies must adopt and maintain an incident response plan	200 penalty units
s 30CP	Responsible entity for a System of National Significance must comply with a notice requiring the entity to undertake a cyber security exercise	200 penalty units
s 34	Reporting entity for, or operator of, a critical infrastructure asset must comply with a direction of the Minister under subsection 32(2)	250 penalty units
s 35AM	In limited circumstances, including where there is a cyber security incident impacting a critical infrastructure asset causing material risk to Australia's national security and the Minister has appropriately authorised the Secretary, a relevant entity must comply with a direction from the Secretary to give information within the period specified in the direction	150 penalty units
s 37(4)	Reporting entity for, or operator of, a critical infrastructure asset must provide information or documents to the Secretary where written notice is provided under subsection 37(2)	150 penalty units

As the civil penalty provisions in the *SOCI Act* are enforceable under Part 4 of the *Regulatory Powers Act*, if the court is satisfied the entity breached the civil penalty provisions, and the entity is a corporation, the court may order the entity to pay up to 5 times the maximum penalty for the provision. For example, failure by a corporation to adopt and maintain a critical infrastructure risk management program under section 30AC is subject to a civil penalty of up to 1,000 penalty units.

There are also two criminal offences under the *SOCI Act*, both punishable by 2 years' imprisonment or fine of up to 120 penalty units or both.

- In limited circumstances, including where there is a cyber security incident impacting a critical infrastructure asset causing material risk to Australia's national security and the Minister has appropriately authorised the Secretary, an entity must comply with a direction from the Secretary to do, or refrain from doing, a specified thing within a specified period under Part 3A of the *SOCI Act*.
- Unauthorised use or disclosure of protected information under Part 4.

The 5 times corporate multiplier in section 4B of the *Crimes Act 1914* applies to these offences. For example, if the entity who breaches an action direction is a corporation, the crime is punishable by up to 600 penalty units.

Enforcement of *SOCI Act* penalties

Home Affairs' current regulatory posture in relation to the *SOCI Act* is that in 2023-24 enforcement action against reporting entities for critical infrastructure will only be for egregious breaches where there has been deliberate, willful noncompliance. The focus of compliance efforts is directed at working with reporting entities to ensure that their submissions and reports are complete and correct. The primary compliance tools in use are education and awareness raising to ensure reporting entities understand and are aware of their obligations. From 2024-25 the regulatory posture is expected to have a stronger compliance and enforcement focus.

Application of the Regulatory Powers Act

As entities' mature under the *SOCI Act* framework, Home Affairs will change its regulatory posture accordingly to monitor and enforce compliance with relevant obligations. To support a change in posture, Part 5 of the *SOCI Act* applies the *Regulatory Powers (Standard Provisions) Act 2014* (*Regulatory Powers Act*) in respect of the penalties under the *SOCI Act*, namely that:

- each civil penalty provision of the *SOCI Act* is enforceable under Parts 4, 6 and 7 of the *Regulatory Powers Act* concerning the seeking of civil penalty orders, enforceable undertakings and injunctions respectively;
- each civil penalty, as well as the two criminal offences abovementioned, is subject to the monitoring and investigation powers in Parts 2 and 3 of the *Regulatory Powers Act*; and
- infringement notices may be issued under Part 5 of the *Regulatory Powers Act* by a Senior Executive Service officer of the Department of Home Affairs appointed by the Secretary, where the officer believes of reasonable grounds that an entity has contravened a civil penalty provision.

Enforcement of civil penalty provisions under Parts 4, 6 and 7 of the *Regulatory Powers Act* would generally be actioned via the filing of legal proceedings by Home Affairs or another relevant Commonwealth regulator against the relevant entity in the Federal Court of Australia or Federal Circuit and Family Court of Australia, with breach of the civil penalty provision determined on the balance of probabilities. A 'relevant Commonwealth regulator' is defined as Home Affairs and any Commonwealth agency specified in rules under the *SOCI Act*—the Department of Defence is currently specified for naval shipbuilding assets, and the Reserve Bank of Australia is specified for critical financial market infrastructure assets that are payment systems.

The monitoring and investigation powers available under Parts 2 and 3 of the *Regulatory Powers Act* include entry to premises by an authorised person from Home Affairs or a relevant Commonwealth regulator, or a person assisting the authorised person, with consent or under warrant for the purpose of monitoring compliance or gathering material that relates to the contravention (or suspected contravention) of an offence or civil penalty provision.

Investigation of the criminal offences would also be able to be undertaken by the Australian Federal Police in accordance with their ordinary powers and procedures, including under the *Crimes Act 1914*.