

CRITICAL INFRASTRUCTURE REFORMS

Six facts you need to know



The Security of Critical Infrastructure reforms are in effect. While you're likely now familiar with the SOCI reforms, here are six things we still think you need to know.

The full package of reforms might not apply to your business, but you still need to care. There's more to the reforms than meets the eye.

The Security of Critical Infrastructure Act (SOCI) breaks down the 11 Critical Infrastructure Sectors into 22 Asset Classes. There are some lengthy definitions underlying each of the asset classes, so the first step is to understand whether your business falls within these definitions and whether you're a responsible entity.

If you're a 'responsible entity', you then need to determine which obligations have been 'switched on' for your asset class. While the Government Assistance Measures apply to all 22 asset classes, the mandatory cyber incident reporting, the Risk Management Program and Asset Register obligations haven't been activated across the board.

However, even if not all of the obligations apply to your asset class, you may still want to engage with the SOCI reforms – find out why below.

Your service providers might now be considered to be critical infrastructure assets due to their commercial relationship with you.

If you're the responsible entity for a critical infrastructure asset and engage a third party to provide services relating to your business critical data, you need to take reasonable steps to inform your provider that they are providing services relating to a critical infrastructure asset. Why? Because they might now be a 'critical data storage or processing asset' due to their relationship with you. This obligation applies regardless of whether any or all of the Positive Security Obligations have been 'switched on' for your asset class. While noting that the intent of the reforms is collaboration rather than enforcement, it would be remiss not to mention that civil penalties can be applied for not meeting this requirement.

On the flip side, as Critical Infrastructure Risk Management Programs will require responsible entities to provide assurance that they're managing risk throughout their supply chain, you or your providers could be identified by other critical infrastructure assets as adjacent systems upon which they depend. This means that the other businesses might also be asking about your risk management settings.

You might now be considered a National Security Business under the Foreign Acquisitions and Takeovers Act (FATA).

If you're a 'responsible entity' per SOCI, or your business is an entity that is a direct interest holder in relation to a critical infrastructure asset per SOCI, the FATA regulations might consider you to be a National Security Business.

It's not just about your own risk appetite. That's why government can intervene in an emergency.

These reforms reflect that critical infrastructure is vital to the nation, which bestows a particular social licence upon CI entities.

As we've seen in recent years, the public expects that the government will have the ability to act in the face of an emergency; that is what these reforms provide. Imagining the immense impacts the nation would experience if your service was compromised should give you an insight into where the government is coming from.

On the bright side, the sharpest of the government's powers (the ability to directly intervene) is subject to stringent safeguards, including a requirement that the Home Affairs Minister obtains the agreement of the Prime Minister and the Defence Minister before it can be enlivened. Still, the existence of this power provides a strong incentive for businesses to take robust action to minimise the likelihood of cyber incidents, even if they're not legally obligated to do so.

If the Minister for Home Affairs is inclined to designate any of your assets as a 'System of National Significance', you will be given time to comment.

The notice will provide a time period to comment – 28 days, or shorter if there are urgent circumstances. You should start thinking now about how you'll respond and what the additional 'Enhanced Cyber Security Obligations' would mean for your business.

All roads lead to cyber, but a purely cyber response won't cut it. This is an opportunity to get your Board on board with prioritising and integrating cyber security.

These reforms are about the intersection of multiple risk factors. While cyber is a key driver, meeting your obligations means thinking about security and resilience from an interconnected, end-to-end perspective. Personnel, physical, cyber and supply chain security all need to play together, not in silos.

Entities are greater than the sum of their parts, so thinking about each of the elements in isolation isn't enough. It would be timely to review whether your governance and other arrangements reflect this, and to take action if they don't.

It's also worth noting that these reforms make it very clear that the government doesn't just see critical infrastructure in terms of hard assets that you can touch, like poles and wires or bridges. Digital infrastructure is also critical infrastructure.

KPMG knows SOCI inside out

We believe we know SOCI better than anyone else in the market. Our team includes leaders who helped develop the SOCI reforms. But more significantly, we're working with regulated entities around Australia and across the 11 critical infrastructure sectors to meet their SOCI obligations, and our experienced core team have been involved in the co-design of the rules and frameworks to bring the reforms to life.

We're passionate about these reforms, and want to support businesses make the most of the opportunity this provides to really focus on your resilience.

We love to talk SOCI. If you want to know more about what the reforms mean to you (including unpacking key definitions such as 'responsible entity' or 'relevant impact'), contact our KPMG professionals below.

Security of Critical Infrastructure Act at a glance

The *Security of Critical Infrastructure Act (2018)* (SOCI) has been significantly strengthened via two tranches of legislative amendments. The first passed in December 2021 and the second tranche came into effect in April 2022.

Together, these amendments expand the reach of the Act from 4 to 11 sectors, and create a framework with the following features:

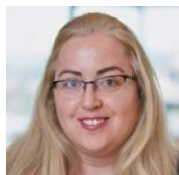
- **A Positive Security Obligation** comprising provision of ownership and operational information to the Register of Critical Infrastructure Assets; mandatory cyber incident reporting obligations within certain timeframes; and development of a Risk Management Program.
- **Government Assistance Measures** that comprise information gather powers, action directions, and intervention powers (these apply to all critical infrastructure assets).
- **Enhanced Cyber Security Obligations** (these apply only to designated 'Systems of National Significance').

This is a VERY high-level snapshot. Let us know if you require a more detailed run-through of the framework.

Contact us



Greg Miller
Partner, Critical Infrastructure
T: +61 2 6218 6625
E: Gmiller3@kpmg.com.au



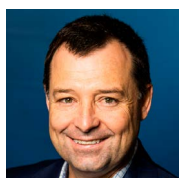
Leah Mooney
Director, KPMG Law
T: +61 7 3237 5437
E: lmooney1@kpmg.com.au



Luke Eason
Partner, Technology Risk & Cyber
T: +61 3 9288 6071
E: lukeeason@kpmg.com.au



Gavin Rosettenstein
National Leader, Third Party Risk Management
T: +61 2 9335 8066
E: gavin1@kpmg.com.au



Peter Beaton
Partner, Governance, Risk & Compliance
T: +61 7 3233 9630
E: pbeaton@kpmg.com.au

kpmg.com/au/soci

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

©2023 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Liability limited by a scheme approved under Professional Standards Legislation.

October 2023. 117692274CORP