CRITICAL INFRASTRUCTURE REFORMS

and the Financial Services Sector

The Security of Critical Infrastructure reforms should now be feeling very real as the grace period ended for the mandatory cyber incident reporting obligation on 8 July. The need to provide ownership and operational information to the Register of Critical Infrastructure Assets is not far behind, with its grace period set to expire on 8 October 2022.

As you prepare to meet the new requirements, here are six things we think you need to know:

The full package of reforms might not apply to your business, but you still need to care – even if you comply with CPS234. There's more to the reforms than meets the eye

The Security of Critical Infrastructure Act (SOCI) breaks down the financial services and markets sector into four asset classes: critical banking assets; critical insurance assets; critical financial market infrastructure assets; and critical superannuation assets. There are some lengthy definitions underlying each of the four asset classes, so the first step is to understand whether your business falls within these definitions and whether you are a responsible entity.

If you are a 'responsible entity' (as per the aforementioned detailed definitions), you then need to determine which obligations have been 'switched on' for your asset class. For example, while the mandatory cyber incident reporting and Government Assistance Measures will apply to all four asset classes, the Risk Management Program and Asset Register obligations only apply to payment systems, which are a subset of financial market infrastructure assets.

This doesn't mean that banking, insurance and superannuation businesses don't need to engage with SOCI. It also doesn't mean that you don't have to worry about SOCI if you are CPS234 compliant. Some reasons why are set out below.

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

If you are the responsible entity for a critical infrastructure asset and engage a third party to provide data storage or processing services in relation to your business critical data, you need to take reasonable steps to inform your provider that they are providing services relating to business critical data of 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 Risk Management Programs will require responsible entities to provide assurance that they are 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 are 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 the government can step-in in an emergency.

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

As we have seen in recent years, the public expects that the government will have the ability to act in the face of an emergency; and that is what these reforms provide. Turning your mind to the downstream and cascading impacts that 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 are not legally obligated to do so.

If the Minister for Home Affairs is minded 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 will respond, and becoming familiar with 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. So personnel, physical, cyber and supply chain security all need to play together, not in silos.

The reforms are about entities being 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 act if they don't.

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

KPMG knows SOCI inside out.

Our team includes leaders who developed the underpinning policy architecture for the reforms while working in Government), as well an experienced core team who have been engaged by the Department of Home Affairs since 2021 to co-design the rules and frameworks to bring the reforms to life.

We are 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 last year, with the second tranche coming 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 are after a more detailed run through of the framework.

Contact us

Martijn Verbree
National Cyber Lead
T: +61 98384049
E: mverbree@kpmg.com.au

Natasha Passley
Cyber Partner, Financial Services
T: +61 2 92735719
E: npassley@kpmg.com.au

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

Carlo Cappuccio
Director, Regulatory & Policy
T: +61 2 6248 1115
E: ccappuccio@kpmg.com.au

KPMG.com.au

July 2022. 918919011CYBER