Dear Stakeholders,

Critical Infrastructure in superannuation – what does it all mean?

GNGB continues to follow the activity of the Department of Home Affairs in the second phase of their Critical Infrastructure consultations.

Despite the draft legislation currently undergoing review by the Parliamentary Joint Committee on Security Intelligence, Home Affairs are powering ahead, developing detailed requirements for the sectors impacted. As the draft legislation stands today, there are a number of questions remaining before an effective efficient Critical Infrastructure framework can be achieved.

Are you in or are you out?

The definition of a Critical Superannuation Asset was initially consulted on in late 2020, but no definition was included in the draft legislation put before parliament. It is clear now that the intent was for the definition to sit within the sector specific rules for the industry. These draft rules were released for consultation on April 23. We presume that this delegation is to enable flexibility as the industry grows and as threats evolve, with Home Affairs able to identify specific assets and bring them in or out of the asset definition without being subject to legislative rigour, purely in the context of

operation of the ‘rules’. The process by which this can be done remains unclear, making it difficult to plan for or assess the impact of the impending requirements.

The proposed rule defining a Critical Superannuation Asset is Registerable Superannuation Entities greater than $20 billion. According to APRA Fund Statistics, as at 30 June 2020, only 24 funds meet that threshold. This is problematic, because regulated entities do not operate in isolation, as recent software compromises have highlighted. The proposed threshold also captures assets that are “used in connection with the operation of a superannuation fund,” which is too broad and ambiguous to be meaningful.

The rationale provided for the asset definition within superannuation is that the critical nature is derived from the contribution of Critical Infrastructure super assets to liquidity and operation of financial markets. This indicates that protection of data is not a focus. This does not capture the full picture, as liquidity and data are inextricably linked by the Data and Payment Standards.

Yes Minister

Asset definitions aside, any organisation within a designated Critical Infrastructure Sector can be subject to ministerial intervention and directed to perform actions where it is deemed necessary to protect a Criticial Infrastructure asset. This has the potential to impact all of us. It is possible that the Australian Cyber Security Centre could be asked to provide resources at short notice to intervene in response and recovery of an incident, the practicalities of which cause anxiety to many. However, as the ACSC point out, this is a power that exists today for those four sectors (electricity, gas, water and ports) currently deemed Critical Infrastructure under existing legislation in place since 2018. We assume that the process, timing and implications of their inclusion such as liabilities, impact

to customer agreements etc have already been defined and addressed. Sharing this information would be helpful to those sectors, such as ours, that are new to this concept and grappling with its implications.

Compounding the issue

Our recent report, Securing the Future, highlighted the challenges with the current regulatory environment, particularly in relation to the fragmented coverage of cyber regulation throughout the end-to-end environment. Currently, regulated entities and their direct service providers are subject to multiple layers of regulation, whilst the remainder of supply chain, and other entities connected with the sector, remain free of even baseline requirements. The approach to critical infrastructure requirements mirrors this pattern – that is, the legislation currently targets only those who are already very tightly regulated as Critical Superannuation Assets (and likely have a high degree of capability to risk assess and manage hazards), leaving the majority of organisations servicing the sector with zero baseline requirements.

Is it a gateway?

A complication for gateways in particular, and likely administrators and member registry providers as well, is that they may be caught by the Critical Data Assets definition that crosses all 11 sectors – defined as “any organisation who processes or stores personal data of more than 20,000 individuals or provides data services to government or a Critical Infrastructure Asset captured under the definition (data sector).”

This definition is built into the current legislation amendment draft, and data sector specific rules are due for consultation later this year. Whilst Home Affairs have signalled that the intent of this definition is to capture data centres and cloud providers, the implication is much broader. Individual assets can be carved out of the definition within the sector specific rules, and Home Affairs has the ability to turn each requirement on

or off by specific asset or sector (see table below). This selective carve out approach is likely to cause more problems than it solves, creating a rabbit warren of regulation coverage rather than a streamlined regulation highway.

It’s not over till it’s over

Parliament stated after the first consultation that they wanted to investigate whether there could be one set of rules that covers all sectors, and a Parliamentary Inquiry to address this is currently underway. However, the development of the draft legislation is continuing in parallel, so this adds additional uncertainty about what those final rules may look like.

Don’t reinvent the wheel

When it comes to developing the rules for our sector, we are encouraging Home Affairs to re-use what already exists. APRA continue to develop CPS234 requirements for trustees in relation to cyber, and we also expect upcoming changes to BCP and Data protection prudential standards. Industry is familiar with the concept of “material outsource provider” and it may be an option to apply this definition to identify assets “used in connection with the operation of a superannuation fund.”

For gateway operators and software providers within superannuation, GNGB’s information security requirements, the ATO’s operational framework and accompanying ABSIA SSAM requirements for Digital Service Providers provide baseline cyber controls which we believe will fulfil the Positive Security Obligation requirements for Critical Infrastructure Assets.

Home Affairs have stated they have an appetite to leverage existing industry practice where effectiveness can be demonstrated, but the degree of leverage is as yet unclear.

GNGB and Critical Infrastructure

At GNGB, we can foresee a situation where partial coverage of participants within the STN as Critical Infrastructure assets complicates our incident response and Gateway Operators' external reporting requirements. In a time where we need to maximise the efficiency and effectiveness of our incident response resources, this is less than ideal. However, the STN is part of a Critical Infrastructure sector and interconnected with many pieces of Critical Infrastructure (depending how these are ultimately defined).

The intention of the legislation is undeniably positive, but there is plenty still to do to make it work as intended for the superannuation sector. Ultimately, the protection of the national interest is an objective we can all agree on – we need to ensure our resources are focussed on the most effective way to achieve this. Consultation on the definition of Critical Assets within Superannuation is open until May 14. If your organisation isn't involved in the discussion, and would like to be, please get in touch.

Not all elements will apply to all entities:

Application of the reforms**

	Entities within Critical Infrastructure Sectors	**Critical Infrastructure Assets**	**Systems of national significance**
Government Assistance	Yes	Yes	Yes
Positive Security Obligations*	No	Yes	Yes
Enhanced Cyber Security Obligations	No	No	Yes

*The obligations under the Positive Security Obligations will need to be 'switched on' (through the making of a rule) for each class of assets, meaning that there will be no regulatory burden experienced by industry

under the Positive Security Obligations until defined within the Rules.

**https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-legislation-amendment-critical-infrastructure-bill-2020