GNGB
GATEWAY NETWORK GOVERNANCE BODY

Gateway Network Governance Body
contactus@gngb.com.au
www.gngb.com.au
27 November 2020

Department of Home Affairs
Critical Infrastructure Centre
ci.reforms@homeaffairs.gov.au

RE: Call for views – Security Legislation Amendment (Critical Infrastructure) Bill 2020 Exposure draft – GNGB Submission

GNGB would like to thank the Department of Home Affairs for the opportunity to provide this submission in relation to the exposure draft. This submission is part of ongoing discussions had with Home Affairs on the exposure draft and we thank Home Affairs for your consideration.

Existing requirements across the Superannuation Transaction Network (STN)

Acknowledging Home Affairs' commitment to leverage existing governance regimes within Critical Infrastructure Sectors, GNGB outlines the existing requirements for Gateway Operators. The interoperability and management of transactions across the superannuation transaction network is governed by a structured framework, inclusive of the following in relation to security, integrity and availability of the Network:

- Principles based requirements within the Gateway Standards and associated Binding Implementation Practices which can be found on GNGB's website here
- Supported by specific information security controls, adapted from the Government's Information Security Manual (STN ISR). The STN ISR is not publicly available however GNGB will provide a confidential copy to Home Affairs for use in understanding the current control landscape across the STN, separate to this consultation response.

Both of these artefacts are reviewed regularly, in line with changes to GNGB's risk assessment of STN information security risks, conducted by GNGB's Security Committee. Gateway Operator compliance to the STN ISR is measured via an annual independent audit report, conducted by an appropriately qualified auditor, as per the policy.

Support for the use of existing frameworks and obligations within the superannuation sector

It is the view of GNGB that the aforementioned framework and its implementation across STN participants would satisfy the Home Affairs requirement for a Positive Security obligation across Gateway Operators and therefore this would not need to be switched on for these entities within the Superannuation Sector. GNGB supports the use of existing APRA prudential standards for Superannuation RSE's as an alternative to switching on the Positive Security Obligation. In addition, we acknowledge APRA's Executive Board Member Geoff Summerhayes' speech on cyber security on 26th November 2020 where he indicates APRA will be "strengthening the chain" to ensure a whole of system approach, recognising the dependencies between ecosystem participants, as opposed to a focus on regulated entities. Together with the introduction of an independent audit for CPS 234 compliance measurement, and additional reporting requirements. It appears APRA has additional plans to address noted risk areas within the industry.

GNGB also supports the alignment of reporting timeframes under existing prudential requirements to reduce implementation complexity. The proposed 12-24 hour timeframe by Home Affairs is shorter than that prescribed by APRA and the Information Commissioner for data breach scenarios. Alignment of notification timeframes would greatly assist the industry to confidently comply.

Management of 3rd parties or service providers in line with Critical Infrastructure obligations

The exposure draft requires clarification as to the management of 3rd parties in an outsourced model, a prevalent business model in the operation of a Superannuation Fund today. It is unclear if the onus is on the regulated entity (RSE) to monitor "critical" 3rd parties and enforce obligations via contractual and operational means or whether those providing services to RSE's, and considered critical, are required to be designated Critical Assets in their own right, and therefore possibly subject to direct obligations.

If the former scenario is the intention of the legislation, it will be imperative to understand in greater detail, what constitutes a critical service provider, as this will likely be applied inconsistently based on regulated entities' risk appetite if left undefined.

The treatment of 3rd parties (and 4th parties) in relation to Ministerial intervention and directed actions also requires further definition. As GNGB understands, the exposure draft is proposing that all entities within the designated sectors may be subject to this obligation, regardless of their designation as a critical asset. This will have a large impact on service providers and potentially their other clients (not the critical infrastructure asset requiring protection). More work is required to define how this process will work, contact points and authorisation channels, so that participants are practiced and ready for this extreme event.

Timeframe for development of sector specific rules and implementation

Finally, GNGB supports the feedback from other industry participants in this consultation, that the proposed timeframe for development of the "Rules" and implementation of obligations across 11 different designated sectors is short. GNGB encourages Home Affairs to consider the number of parties that possibly could be subject to the obligations imposed and to allow appropriate lead time for changes to organisations' policy and practices in relation to all hazards resilience.

Kind Regards

contactus@gngb.com.au

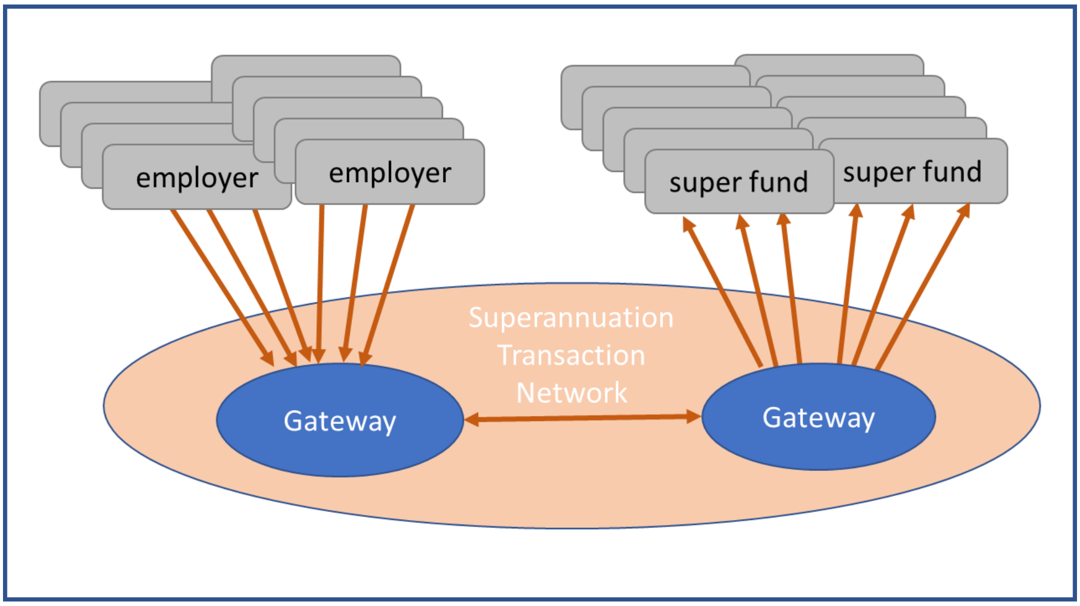
About us

The Gateway Network Governance Body Ltd (GNGB) was established in 2016 as an industry owned, not-for-profit governance organisation whose main purpose is to manage the security and integrity of the Superannuation Transaction Network (STN).

The STN is the data infrastructure that connects employers to the superannuation funds of their employees. It is the digital data messaging network over which superannuation transactions, such as rollovers and contributions, are sent between employers and funds via their technology service providers, who are known as Gateway Operators. The STN is currently connected to all Australian Prudential Regulation Authority (APRA) regulated superannuation funds and will incorporate Self-Managed Superannuation Funds (SMSFs) from March 2021. Since July 2018, over 694,000 employers have transacted over the network with an average of approximately 83 million data transactions per year. There are currently nine Gateway Operators within the STN. Since 2016, GNGB has been successful in the implementation of governance across the STN, specifically:

- Undertaking initiatives to promote the security, **efficiency and effectiveness** of the STN
- **Monitoring compliance** with the Gateway Standards, together with developing and providing oversight of specific Information Security Requirements
- Managing **new entrants and exiting gateway operators** to the network
- **Engaging with key stakeholders** in Government and industry
- Coordinating **change management** activities as legislation and associated instruments change, including the facilitation of member forums and opportunities to test and validate interpretation of legislative change, emerging technology and other developments.

It is important to note that the STN is defined by the boundaries around which Gateway Operators interact with each other, in relation to current governance scope. The STN is a four corner model of data exchange, with the STN Governance framework coverage extending across corners two and three. The below diagram outlines scope of the current regime in the example of contributions messages:



GNGB Stakeholders

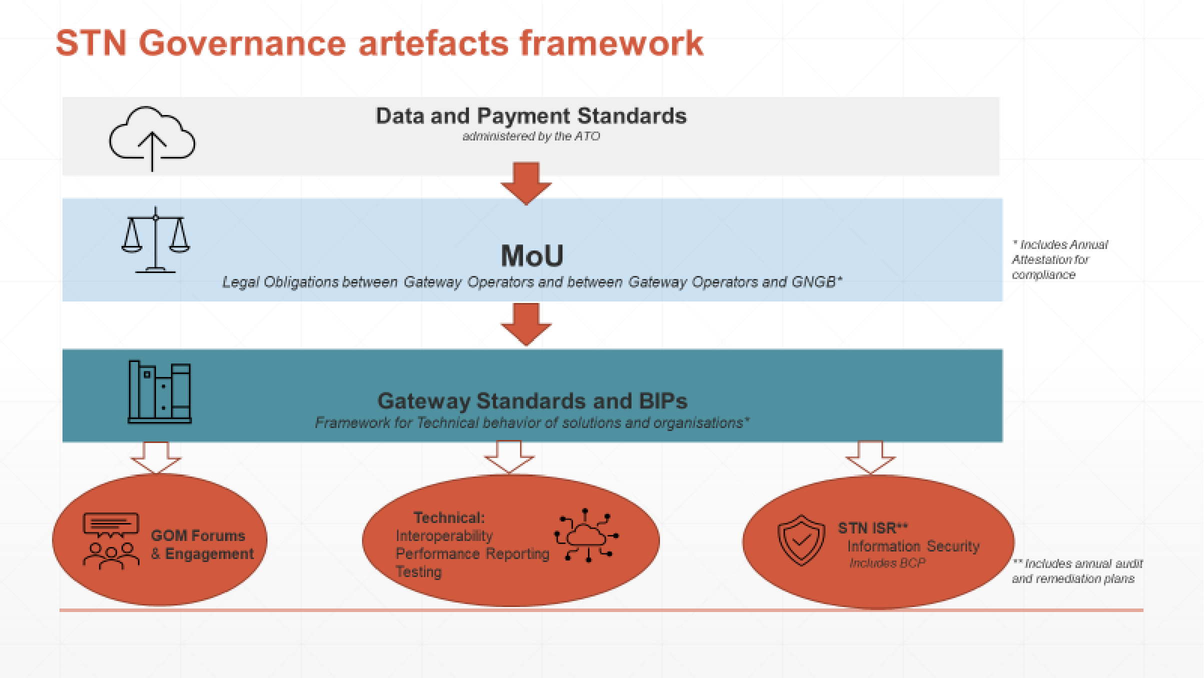
The accredited Gateway Operators within the STN range from large bank supported organisations or subsidiaries, to small business operators and fintechs. GNGB is experienced in guiding organisations across the maturity spectrum to identify, develop and implement solutions within a highly regulated environment.

In addition, GNGB's co-sponsor members (i.e. the founders of the organisation) are involved in the design and development of GNGB and are also represented on the GNGB Board. Co-sponsor members include:

- ABSIA – Australian Business Industry Software Association
- ACCI – Australian Chamber of Commerce and Industry
- AIST – Australian Institute of Superannuation Trustees
- ASFA – The Association for Superannuation Funds of Australia
- FSC – Financial Services Council

Current STN Governance Framework

The current governance framework consists of an MoU binding Gateway Operators to each other and to GNGB in respect of their obligations. The MoU outlines compliance with Gateway Standards (framework for interacting) and Information Security Requirements (STN ISR), largely based on the government's information security manual controls.


STN Governance artefacts framework

Data and Payment Standards
administered by the ATO
MoU
Legal Obligations between Gateway Operators and between Gateway Operators and GNGB*
* Includes Annual Attestation for compliance
Gateway Standards and BIPs
Framework for Technical behavior of solutions and organisations*
GOM Forums & Engagement
Technical:
Interoperability
Performance Reporting
Testing
STN ISR**
Information Security
Includes BCP
** Includes annual audit and remediation plans