Gateway Network Governance Body
contactus@gngb.com.au
www.gngb.com.au
16 September 2020

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

RE: GNGB Submission to the Home Affairs call for views on Protecting Critical Infrastructure and Systems of National Significance

The Gateway Network Governance Body (GNGB) welcomes the opportunity to make this submission to the *Department of Home Affairs in relation to consultation on protection of critical infrastructure in Australia*. GNGB is an industry-owned governance body which oversees the data infrastructure known as the Superannuation Transaction Network (STN). It is with this experience GNGB provides this submission to the consultation paper, as well as the issues raised in the Banking and Finance workshop as part of the department's consultation process. GNGB's response is focused on the STN and the proposed critical infrastructure protections in a superannuation context.

A summary of GNGB response to the Department of Home Affairs' questions, focusing on those areas raised for discussion in the Banking and Finance Sector workshop is outlined below, followed by an Overview of GNGB and the STN, together with an expanded response as Appendix 1.

- ✓ Definition of critical infrastructure within the Banking and Finance Sector should be refined to provide greater clarity. A broad range of entities play a part in the provision of financial services, and the goal should be to understand criticality thresholds of those functions. The APRA concept of 'material outsource providers' may be relevant here. The STN would not be included in the current list of assets designated by the consultation material, however GNGB believes the STN is critical data infrastructure underpinning superannuation by delivering member data to super funds and should therefore be designated as Regulated Critical Infrastructure.
- ✓ Current regulatory environment is complex and made up of multiple obligations on licensees and patchy coverage along the data value chain between superannuation funds and employers paying super on behalf of their employees. More should be done to ensure a baseline level of regulation, based upon existing regimes, is applied to all participants in the value chain.
- ✓ Implementation of the PSO in the STN – entities within the STN are subject to multiple layers of governance, including GNGB's own governance framework and the ATO's Operational Framework. Entities providing services to super funds are also subject to the requirements of CPS234 as they relate to third parties. GNGB expects there would not be a need to extend additions to this governance regime in order to satisfy Critical Infrastructure requirements however any tweaking required to existing regulation can be incorporated into the GNGB governance framework to ensure consistent application across the STN.
- ✓ The role of government in threat sharing and incident response is critically important to the STN in particular, and the superannuation sector more broadly. GNGB sees this as a crucial to maintaining the integrity of the superannuation ecosystem, and of growing importance as a key tool in cyber defence. It is anticipated the resources and capability within government applied to

threat monitoring, analysing and reporting would be superior to those deployed by individual organisations within superannuation, benefitting the entire sector. In addition, government has the advantage of a consolidated view of the threat landscape, and a pivotal role to play in collection, analysis and dissemination to appropriate parties. Such an approach would improve overall sector defences within the threat environment and improve situational awareness for all entities. Coordination of an incident response across sectors or for those entities who cannot provide sufficient defence would be of benefit.

- ✓ Directed action or direct intervention by government can be seen as helpful, however will have an impact on commercial considerations. GNGB supports further dialogue in regard to the proposed powers, including in-principle agreement for criteria to be met prior to invocation, and detailed scenario analysis, as well as ensuring an adaptable, risk-based approach with the ability to respond to changes in criminal activity and the nature of threats.

GNGB welcomes further dialogue in relation to Home Affairs consultation, please do not hesitate to contact us for further information.

Kind Regards

contactus@gngb.com.au

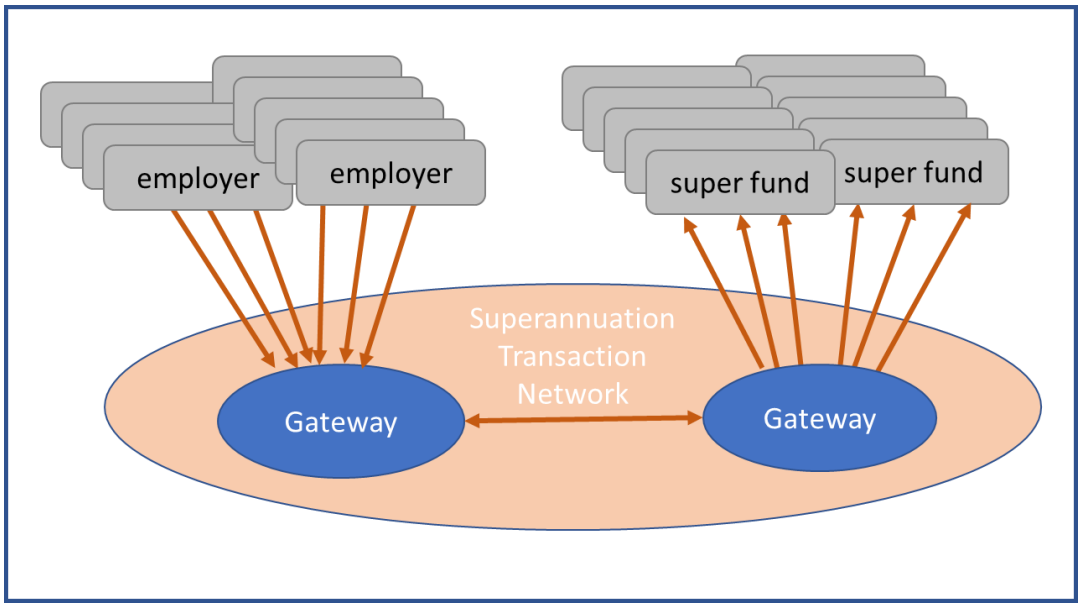
About us

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

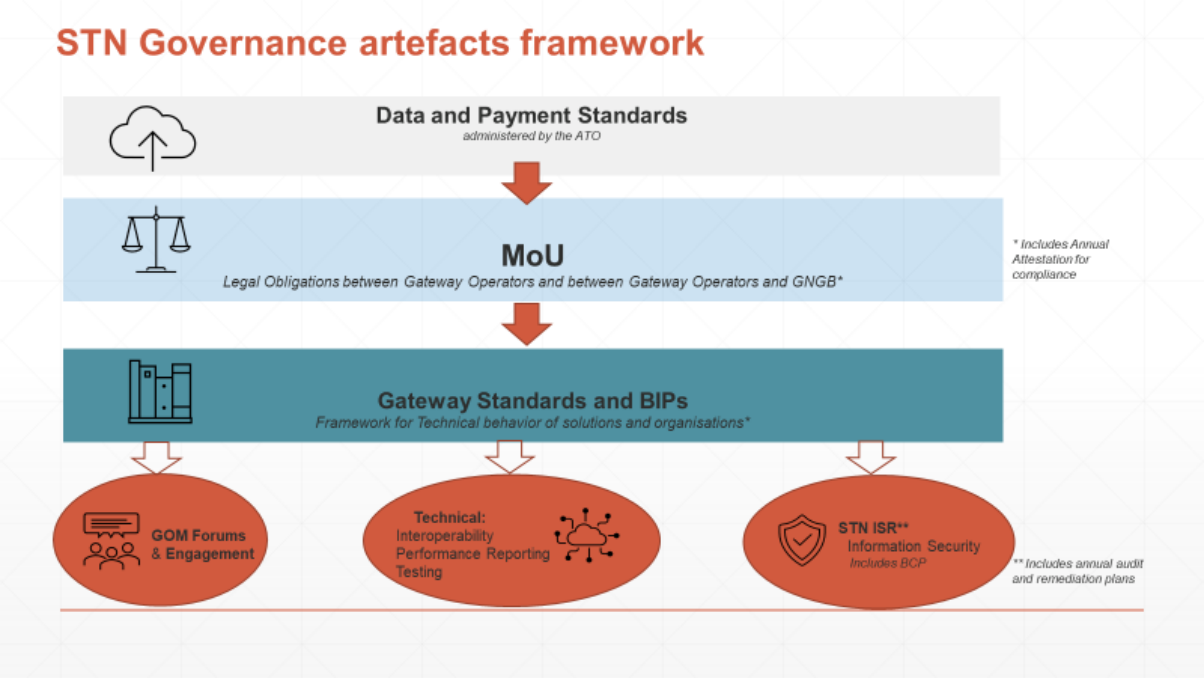
The accredited Gateway Operators within the STN range from large bank supported organisations or subsidiaries, to small business operators and fintechs. GNGB is experienced in guiding organisations across the maturity spectrum to identify, develop and implement solutions within a highly regulated environment.

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.



GNGB Detailed Response

Background and Context

Cyber Strategy 2020 was released on August 6th, naming a key initiative as "Protecting and actively defending the critical infrastructure that all Australians rely on, including cyber security obligations for owners and operators." This aligns with the submission GNGB made in October 2019 in response to the governments' call for views on Cyber Strategy 2020 where we stated that "Government should widen the traditional definition of 'Essential Services' to include key financial service networks, such as the Superannuation Transaction Network (STN) and Single Touch Payroll (STP) network."

Shortly after Cyber Strategy 2020 was published, Home Affairs released a consultation paper on Critical infrastructure seeking feedback on their proposed expansion to new sectors as well as requirements for critical infrastructure owners and operators.

GNGB are pleased to provide the following response for consideration by the Department of Home Affairs.

1. Definition of critical infrastructure

GNGB supports the expansion of the current definition of critical infrastructure. In particular, the expansion to superannuation, within the Banking and Financial Sector, in relation to data and cloud infrastructure assets. The definition stated in the Banking and Financial Sector workshop material is too broad to enable a clear understanding of the coverage of entities within superannuation. Whilst superannuation funds are connected directly to their members as consumers of their products, the superannuation ecosystem is broad and includes many organisations along the value chain including employers, their service providers such as accounting, tax agents, payroll services, clearing houses and gateway operators. The latter of these may also provide services to superannuation funds together with custodians, administrators, call centres and mail houses. 'Financial services' is a broad term and "entities involved in the delivery of..." could apply to many organisations. APRA utilises the term "material service providers" to capture applicable service providers for APRA-regulated entities and this may be a good reference point. GNGB notes that the definition of material, whilst guidance is provided in some instances, is largely left to the regulated organisation to determine, based on their solution context and operating model.

2. Entities covered by the category of regulated critical infrastructure

The Superannuation Transaction Network and the Gateway Operators participating within the network would not be included in the list of entities covered by the categories listed in the Banking and Finance workshop material as it stands. RSEs refers only to the Trustee entity of the superannuation fund within the sector. GNGB suggests amending this list such that the STN is included.

The STN is a key network enabling employer contributions and super fund rollovers to be exchanged between funds and employers. Both stakeholder groups depend upon the STN to keep their data safe, secure and available, to enable their legislative obligations and deadlines in relation to the superannuation Data and Payment standards. If the STN were to be compromised to the extent of failure to exchange messages, the following consequences would arise:

- Inability for super funds to allocate member contributions to accounts
- Liquidity inputs into funds in the form of contributions and/or rollovers would likely be delayed/halted

- Potential for sensitive data such as member credentials, TFNs, DOB, address, salary and employment information to be exposed or stolen

Should the department of Home Affairs deem the STN applicable for inclusion as an asset within critical infrastructure definition, consideration needs to be given to the fact that Gateway Operators are a diverse set of organisations in terms of size, complexity and client types. GNGB has demonstrated experienced in navigating the balance of baseline data and controls integrity and diverse participant organisations and would be supportive of leveraging the existing regulatory environment rather than imposing additional requirements.

3. Level of existing regulation and governance for the STN

The existing regulatory environment across superannuation is complex and challenged by the interdependencies of various technology solutions within the data supply chain of the superannuation ecosystem. No single regulator covers all entities within the data supply chain, and some stakeholder groups are devoid of formal regulation whilst others are covered by multiple regimes.

Super funds are responsible for the safety of their member data and employers are required to comply with superannuation guarantee obligations, however both funds and employers may solicit or make use of multiple service providers in the execution of their obligations. These service providers, which many include administrators, accounting software, payroll providers, clearing houses, are often unregulated.

APRA is responsible for fund regulation and has, with the introduction of CPS 234, sought to cover information security obligations relating to third parties directly contracted by super funds in the handling of member data.

The STN is regulated by the ATO in terms of the Superannuation Data and Payment Standards 2012 as amended made under subsection 34K(3) of the Superannuation Industry (Supervision) Act 1993.

The governance of the STN, being the role for which GNGB is provided under the Australian Prudential Regulation Authority Act 1998 ("APRA Act"). In 2015, the STN information security requirements were developed for Gateway Operators participating within the network and these have been subject to continuous improvement. They remain based on the Government's information security manual (ISM) controls.

Subsequent to this, effective 2019 December, the ATO also required digital service providers interacting with their superannuation services to comply with the Operational Framework also outlining security requirements.

The challenge for superannuation is ensuring the data value chain, end to end, has a baseline level of security.

Discussion from the industry workshop indicated that in Banking and Finance, CPS234 or the CPS23x series may be a good basis from which to satisfy Home Affairs requirements of the Positive Security Obligation required of entities/systems identified. GNGB supports the use of existing regulatory regimes to deliver desired outcomes and does not see that RSE's and their material service providers require any additional regulations.

GNGB is regularly benchmarking the governance framework across the STN to other industry guidance and prudential standards, to ensure our Gateway Standards and Information Security Requirements align to the industry's expectations. If existing regulatory frameworks were tweaked to capture Critical Infrastructure Requirements, GNGB could incorporate these additions into the STN governance framework where applicable.

4. Are there factors in addition to interdependency with other functions and consequence of

compromise that should be considered when identifying and prioritising critical entities and entity classes? Interdependencies and consequences of compromise are good indicators to consider when determining critical assets, however GNGB would also consider the risk (likelihood) of compromise when understanding how to prioritise resources. The method for identifying and prioritising critical entities must enable flexibility to consider additional entities or remove entities over time, as risks and functions of critical entities evolve and new sectors emerge or existing sectors recede.

5. What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?
What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?
What are the barriers to owners and operators acting on information alerts from Government?
What might this new TISN model look like, and what entities should be included?
The STN would benefit from an enhanced threat information sharing model with government and GNGB has, together with superannuation industry associations, proactively led in discussions with agencies regarding the ability to share fraud and threat material more broadly. However, these discussions did not reveal a result in ownership of this initiative within government.

Threat sharing is a critical foundation in maintaining the integrity of the superannuation ecosystem. It would be of benefit to the STN for government to share information regarding:

- indicators of compromise for threats targeting superannuation or pension networks abroad or locally perpetrated by state-based actors or criminal gangs;
- timely notification of known software vulnerabilities for solution components utilised in the superannuation ecosystem.

It is anticipated the resources and capability within government applied to threat monitoring, analysis and reporting would be superior to those deployed by individual organisations within superannuation and the sector at large would benefit. In addition, government has the advantage of a consolidated view of the threat landscape and a pivotal role to play in collection, analysis and dissemination to appropriate parties, to uplift the overall sector defences within the threat environment and improve situational awareness for all entities.

Gateway Operators are accountable for monitoring their own operating environments for prevention and detection of threats to information security. GNGB would be open to working with government to find a practical solution to how threats may be shared with government if that would be of value. Any cost implications are unknown at this point in time and are dependent on the method/timeliness of sharing required. For threat sharing to be mutually beneficial, it is critical to separate information collection for threat sharing purposes from information collection for compliance or supervisory purposes.

We have not identified any barriers to Gateway Operators or GNGB acting on information alerts from government, however we acknowledge that all entities would need time to change their business processes and technology to implement a threat sharing model effectively into their organisations.

All entities within the designation of critical infrastructure should benefit from the TISN model, not just those designated as systems of national significance. It is however important to strike a balance between general threat information being shared by all and specific sector or function threat

information which may be more valuable and effective in protection against actual threats for an individual organisation or sector.

6. What are the common threats you routinely prepare for and those you have faced / experienced as a business?

Information security is at the heart of what we do as GNGB and this if reflected within our governance framework including:

- specific Information Security Requirements for all network participants, annually audited by an independent auditor, together with ISO27001 accreditation.
- Cyber threats – incident response planning including annual simulation of cyber incident scenarios as a network to practice network wide incident response, threats simulated include ransomware, data breaches, DDOS attacks
- Physical threats – annual business continuity planning and testing to enable practiced response to natural disasters or other threats to availability of hardware and premises
- Threats to our key people including that of the pandemic and others via policy and contingency planning

7. Impacts to the STN / GNGB

Should the department of Home Affairs incorporate the STN into the Regulated Critical Infrastructure entities, the consultation material outlines what would be applied. This is shown as two high level obligations:

- Positive security obligations
- Government advice and direct actions

Government advice and direct actions encompasses the proposal from Home Affairs to enable the Minister to make decisions on behalf of individual entities, should it be deemed required, in relation to prevention, defence or intervention in the response to a particular event, or for the government to take direct action regarding incident response. Whilst we acknowledge this is likely to be in extreme circumstances where national security is at stake or cross sector dependencies exist, this power should be considered carefully, with regard to commercial implications of direct action taken by government. GNGB would support further dialogue regarding these powers, including in-principle agreement on criteria to be met prior to invoking these powers, together with rehearsals or simulations of the situation where these powers may be invoked, in order to test coordination of this type of response. It is difficult to anticipate where these might apply within a superannuation context. GNGB recommends including consideration of an entity's ability to opt into this type of government support based on recommendations from ASD or appropriately qualified cyber specialists.

Tangible benefits to the STN that can be seen as part of tCritical Infrastructure are thought to be largely in the area of cyber preparedness , including threat information sharing, playbook development and the potential for government assistance during the management of a threat in extreme circumstances or in the case of cross sector threats.

Costs to the STN / Gateway Operators / GNGB

Without understanding further the requirements that may be involved in compliance to or reporting of compliance to the PSO, it is difficult to estimate impact to costs of GNGB or individual Gateway Operator entities. Current compliance costs for Gateway Operators, inclusive of annual independent audit, range approximately between $10,000 and $100,000.