GNGB
GATEWAY NETWORK GOVERNANCE BODY

Jan McClelland AM
Chair
Gateway Network Governance Body Ltd
Email: [redacted]

31 October 2019

The Hon Peter Dutton MP
Minister for Home Affairs
By submission

Dear Minister,

Thank you for the opportunity to submit a response to A Call for Views into Australia's 2020 Cyber Security Strategy. The Gateway Network Governance Body (GNGB) strongly supports the view that cyber security and indeed, cyber resilience, is critically important. We are pleased to enclose detailed responses in Appendix A.

As the Governance Body across the Superannuation Transaction Network (STN)* we are acutely aware of the importance of security and education on this issue. As an illustration of the importance the GNGB places on cyber security, we have established a Security Committee of our Board to directly address the issue of cyber threats, increase the awareness of mitigation strategies and play a leadership role in the superannuation industry. The activities of the Security Committee culminated earlier in 2019 in the simulation of an STN-wide cyber incident and response. I enclose our report on this exercise as Appendix C.

The GNGB submission views can be summarized at a high level into the following themes:

1. The leadership role of Government in promoting awareness and understanding of cyber security, development of cyber resilience capability and incorporation of cyber security standards in regulatory frameworks is critical.
2. Cyber protections need to be viewed in the context of the digital ecosystem, with dependencies between sectors, entities and individuals.
3. Greater assistance is required for Small to Medium Enterprises (SME's) which are at risk and often less well equipped in cyber resilience, introducing potential risk to the financial and data ecosystem.
4. The Superannuation Transaction Network (STN) directly or indirectly interacts digitally with many employers in Australia, approximately 694,000 individual ABN's have transacted via the

network since July 2018. STN practices and policy can have an important role to play with uplifting the cyber resilience of SMEs.

5. Government has an important role to play in facilitating access to Managed Security Service Provider (MSSP) capabilities, to help reduce the burden of protection for SMEs. In addition, the research is unequivocal in its conclusions that the most effective protection against cyber threats is the sharing of threat intelligence. There is potential for Government to play a centralised role facilitating the delivering of this capability.
6. Government should widen the traditional definition of "Essential Services" to include key financial service networks and payment platforms, such as the Superannuation Transaction Network (STN), to take into account the potential for "Unrestricted Warfare".

Australia has an opportunity, with appropriate Government support to take a leading global position with cyber security and education creating a baseline for resilience against ongoing threats.

We would welcome the opportunity to be involved in further discussions with the government and industry on this important issue. Should you require any further information please do not hesitate to contact the GNGB Executive Officer, Michelle Bower on [redacted] or the Chair of the GNGB Board Security Committee, Ian Gibson on [redacted]

Yours sincerely,

[redacted]

Jan McClelland AM
Chair
Gateway Network Governance Body Ltd.

*Overview of the STN and GNGB provided as Appendix B.

GNGB
GATEWAY NETWORK GOVERNANCE BODY

Appendix A

GNGB Detailed Responses to A Call for Views: Australia's 202 Cyber Security Strategy

1. What is your view of the cyber threat environment? What threats should Government be focusing on?

The cyber threat environment is becoming more complex and pervasive, and while there are elements that might be location specific, it is international in nature. The ability for cyber threats to infiltrate the daily lives of Australians is becoming greater with the increasingly digitised landscape within which all Australians operate, e.g. Internet of Things and Artificial Intelligence (AI) assisted devices

As a consequence of the broad and complex cyber threat environment, the focus needs to be on a broad range of areas particularly standards within consumer products, educations and skills development, information sharing and collaboration both within our sector ecosystems but also with our international peers. The danger of focusing on specific areas is that it creates pockets of vulnerability, so a broad and balanced approach is necessary, due to the interdependencies of the digital landscape.

Historically cyber security has been seen as a technology issue. There is increasing awareness that it is a business issue. APRA's recent release of CPS 234 make this clear by ensuring directors are responsible and that protections exist on an end to end basis, recognising the importance of third party suppliers' cyber resilience.

2. Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

GNGB agrees with the Government's assessment of the current responsibility allocation for managing cyber risks in the economy. When it comes to cyber resilience, the current focus is on the end users, however this ignores the externalities associated with this approach. The increasing interconnectedness of organisations means that cyber security is less about individual entities or users and more about the ecosystem. The implication is that any cyber security strategy needs to take account of the importance of protecting the ecosystem, the broader environment and recognise that the action of one entity has flow-on consequences for others.

Any regulated entity would have its own safeguards and/or be developing a capability, however the governance around the ecosystem and the recognition of dependencies between organisations is also critically important. There is currently a gap across sectors and entities. For example, who orchestrates identification and assessment of threats when there are multiple interconnected networks – who coordinates the recovery of the ecosystem? Within the STN, the collaboration within our network, under the guidance of the GNGB allows us to fill that gap, however across essential services, both traditional and non-traditional, there is currently limited collaboration that we are aware of.

Government has a multifaceted role with cyber security:

a. As a Business that needs to protect its own assets
b. As a creator of demand for new services and a driver for the development of skills / capabilities
c. As a setter of cyber security standards that different products and service must adhere to e.g. with Internet of Things (IoT) devices
d. As a reference for advice and information sharing, facilitating collaboration and thought leadership
e. As a policing authority to detect and prosecute cyber criminals
f. As a resolution for commercial market failures such as being a service provider where the market has failed, for whatever reason, to address a need

3. Do you think the way these responsibilities are currently allocated is right? What changes should be considered?

Government has a strong role to play in standard and law setting across consumer goods and services and essential networks in relation to cyber resilience.

Government, in collaboration with industry, can play a much broader role with a view to protecting the digital ecosystem and sharing intelligence that can aid in greater protection for all users.

4. What role should government play in addressing the most serious threats to institutions and businesses located in Australia?

Government has a multifaceted role with cyber security:

a. As a Business that needs to protect its own assets
    - ensure that Government assets are protected from cyber threat
    - act as a model of cyber security
    - work within its ecosystem to help all participants to mitigate cyber threats
b. As a creator of demand for new services and development of skills / capabilities
    - Through its education responsibility (both Secondary and Tertiary) to promote the development of security skills and capabilities
    - As an enabler, between industry and educators with a view to build world leading skills development frameworks
c. As a setter of cyber security standards that different products and services must adhere to e.g. with Internet of Things (IoT) devices
    - Many users of services are ignorant of the cyber security implications or do not have the capabilities to adequately assess them

- APRA's CPS 234 is a good example of a regulator setting a mandatory minimum cyber security requirement, however it only applies to APRA regulated entities and their service providers
- Cyber insurance terms and conditions vary significantly, so what is being covered and the risks being borne by the Insured are often unclear

d. As a reference for advice and information sharing
   - Stay Smart Online is a good example of this, however it is not widely promoted and or known about
   - Creating a framework to encourage businesses to digitalise and then to get the basic "cyber" hygiene's right e.g. digitalising, migrating to the cloud, leveraging MSSPs
   - Providing or facilitating a threat intelligence sharing capability to enable businesses' proactive knowledge of criminal activity to better protect against such threats

e. As a policing authority to detect and prosecute cyber criminals
   - Government has a critical role in dealing with state sponsored agents and organized cyber criminals

f. As a resolution for market failures such as being a service provider where the market has failed, for whatever reason, to address a need
   - As a facilitator of access to cyber security managed services for those small to medium enterprises (SMEs) who would otherwise not have that access
   - The uptake of cyber insurance is still low, while the potential consequences for business, especially small to medium businesses, can be catastrophic. The immaturity of the cyber insurance market means obtaining cyber insurance can be difficult and costly; that the terms and conditions vary significantly between providers also makes comparisons difficult;

5. How can government maintain trust from the Australian community when using its cyber security capabilities?

The role that government plays is not well understood

Government has focused its attentions on the "traditional" Essential Services, however the definition needs to be broadened to incorporate new and emerging networks with the potential to cause significant disruption if they suffered a cyber-attack, state sponsored or from other actors, e.g. financial services and data networks such as the STN, Single Touch Payroll (STP), eInvoicing, the New Payments Platform (NPP) and others.

6. What customer protections should apply to the security of cyber goods and services?

See answer to Question 8e.

7. What role can Government and industry play in supporting the cyber security of consumers?

    a. Promoting the development of cyber security skills and capabilities especially at tertiary institutions

    b. Facilitating Managed Security Service Provider (MSSP) capabilities to lower the cost and capability burden on small and medium business e.g. making The Digital Identity Framework (TDIF) as a service available to trusted third parties

    c. Creating the demand to underwrite developing consumer oriented cyber security products and services

8. How can government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

    a. Promoting developing cyber security skills and capabilities especially at tertiary institutions

    b. Facilitating Managed Security Service Provider (MSSP) capabilities to lower the cost and capability burden on small and medium business e.g. making The Digital Identity Framework (TDIF) as a service available to trusted third parties

    c. Creating the demand to underwrite developing consumer oriented cyber security products and services

    d. Engaging with SMEs with specifically targeted assistance

    e. Introducing the cyber equivalent of an Energy Rating. This would re-assure consumers that the goods and services bearing the “Cyber Rating” has a minimum level of cyber security. It also provides appropriate incentives to companies to strengthen their cyber capabilities and to use secure service providers

Star Rating	Illustrative Compliance Definition
1	• Held the 1-star rating for 12 months; AND • No security incidents in the past 12 months; OR • Held the 2-star rating for 12 months or more; AND • 1 or more security incidents in the past 12 months
2	• 1 international recognised ISO standard; AND • 1 Australia security standard (e.g. Operational Framework)
2.5	• Held the 2-star rating for 12 months or more; AND • No security incidents in the past 12 months OR • Held the 3-star rating for 12 months or morel AND • 1 or more security incidents in the past 12 months
3	• 1 international recognised ISO standard; AND • 2 Australian security standards (e.g. Operational Framework and the STN ISM)
3.5	• Held the 3-star rating for 12 months or more; AND • No security incidents in the past 12 months
4	• Held the 3-star rating for 12 months or more; AND • No security incidents in the past 24 months

* If the company can be upgraded to a new star rating due to compliance to additional security standards (e.g. 1 to 2 or 2 to 3 etc.) but has had a security incident in the past 12 months, the new star rating will not take into effect until 12 months have passed since the last security incident

9. Are there functions the government currently performs that could be safely devolved to the private sector? What would the effect(s) be?

This question is intentionally left blank.

10. Is the regulatory environment for cyber security appropriate? Why or why not?

We agree with the Government's view that the regulatory environment for cyber security is inconsistent across sectors. This approach is consistent with an immature regulatory environment where the initial focus has been on the highest risk areas. A more consistent approach is needed due to the proliferation of digital goods and services delivering an exponential increase in points of access for malicious actors.

11. What specific market incentives or regulatory changes should government consider?

We refer to the case study on page 12 of the Call for Views document. GNGB believes a similar role to the European *Directive on Security of Network and Information Systems* (NIS Directive) could be introduced in Australia with particular reference to the introduction of supervisory

powers over essential services (both traditional and non-traditional) including ongoing governance of implementation of cyber security standards.

Such a supervisory role also allows end to end visibility of emerging threats and latest developments which would enable a platform for information sharing and collaboration.

12. What needs to be done so that cyber security is 'built-in' to digital goods and services?

We agree, ideally, digital products and services should have security built in 'by design' so that users do not need to have any expert knowledge in order to differentiate and select products aligned to their individual risk appetites. By developing standards and certifying goods and services against those standards, the Government could be providing a simple comparison point for consumers to make informed decisions, without expert knowledge on information security requirements.

These standards could then be specified as part of tendering requirements (initially via government procurement) and subsequently adopted by industry. This would be aligned to the Government's previous practices of leading by example.

Greater awareness by consumers would drive demand for higher rated cyber safe goods, which can be facilitated, in part, by government advertising.

13. How could we approach instilling better trust in ICT supply chains?

This question is intentionally left blank.

14. How can Australian governments and private entities build a market of high quality security professionals in Australia?

Two pathways are available to enable the building of high quality security professionals:

- Education – working with tertiary education institutions to provide clarity around qualifications and skills required for a career in information security. Greater definition of careers available in the field and where the opportunities, and the demand for skills exists.
- Attracting talent for other industries/other regions – building the profile of the Australian cyber capabilities and demonstrating leadership in this area will serve to attract talent to the roles required

15. Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

Insurance can help policy holders prevent, respond and recover from cyber incidents. The market for cyber insurance remains relatively immature which can result in the following issues arising:

- Lack of standard terms of coverage in cyber insurance contracts

- Small risks pools to understand the risk levels and inconsistency in estimating risk (and therefore premiums)
- Difficulty in obtaining cyber insurance. In some case companies are applying for cyber insurance and are unable to get coverage
- Increasing premiums for those companies able to get cyber insurance coverage
- Mitigation activities undertaken by organisations against cyber risks are not well understood and therefore often not considered by insurers as important in assessing the overall risk profile.

Government could give consideration to introducing a cyber insurance scheme similar to Workers Compensation that provides coverage to all businesses against a catastrophic cyber incident. The Government scheme could be administered by industry and established as a basic coverage scheme with the option for industry to provide top-up / customised coverage, similar to the way compulsory third party car insurance is implemented.

16. How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

Increased education and the raising of awareness with users, especially students (both secondary and tertiary) and SME's, as well as those less familiar with the digital environment, such as the elder generations.

17. What changes can government make to create a hostile environment for malicious cyber actors?

The main focus of government efforts could be on:

- Detection and policing – education of businesses and individuals so that they are equipped to identify issues early and develop monitoring processes and policies to protect their own environments and those they integrate with
- Ensuring mandatory reporting – where a breach has occurred, or is highly likely to have occurred, introduce a mandatory reporting mechanism to government
- Facilitation of active information sharing, possibly on an anonymous basis to encourage participation and remove commercial impact.

18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

Participation in proactive threat intelligence sharing increases the identification of cyber risks. In addition, remediation is a form of business continuity planning. The STN recently underwent testing of a simulated cyber-attack scenario to familiarise participants, including Gateway Operators, the Australian Taxation Office (ATO) and GNGB with the steps required to remediate a breach of the network and build cyber resilience. We enclose a copy of the report on the Cyber Incident Exercise conducted and the outcomes, as Appendix C.

19. What private networks should be considered critical systems that need stronger cyber defences?

To date, most focus has been on the "traditional" Essential Services. While appropriate, it ignores the changed reality that many secondary networks now have the potential to create significant disruption if they were subject to a cyber incident.

The concept of "Unrestricted Warfare" where common things, such as the reliance on technology, are leveraged to become weapons with which to engage in war, requires the concept of essential services to be widened.

These "secondary networks" may include, but are not limited to:

- Superannuation Transaction Network (STN)
- Single Touch Payroll Network (STP Network)
- E-invoicing network
- New Payments Platform

20. What funding models should government explore for any additional protections provided to the community?

If government needs to provide ongoing and sustainable services to the owners of critical systems, then the cost may need to be recovered through direct charges or other alternative funding models, rather than relying on general taxation revenue.

The funding model appropriate to each network may vary, so tailored funding models should be investigated.

21. What are the constraints to information sharing between government and industry on cyber threats and vulnerabilities?

Information sharing is acknowledged as one of the best defenses against cyber-crime, yet it occurs only in limited situations. Some of the issues preventing improved information sharing include:

- Varying involvement across several government agencies
- Concerns about confidentiality
- Concerns about the commercial implications of the required level of transparency

To successfully encourage threat intelligence sharing, a centralised solution must be able to consume and validate the data being submitted by solution providers under attack, de-identify the source of the intelligence and broadly distribute attributes / characteristics of emerging threats.

22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

A lack of cyber awareness drives poor consumer outcomes as cyber resilience is not a feature currently used to evaluate consumer products on a large scale. Increasingly, cyber risks affect consumers with the abundance of readily available vulnerable products. Consumers need to understand the importance of cyber security when selecting products and driving demand.

One option is to include cyber security awareness in schools. Currently schools teach computer literacy but that does not include the protection of information and the consequences of misuse or gaps in cyber protection. The development of awareness of cyber security and engagement in the development of strategies and solutions among the next generation is critical for the future, as they become both consumers and decision makers.

From a commercial perspective, APRA's recent introduction of CPS 234 is a positive step as it formalises cyber security as a business issue that company directors of APRA regulated entities need to engage with. It also acknowledges the dependencies between technologies and operating environments by including responsibility for third party service providers.

23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

This question is intentionally left blank.

24. What are examples of best practice behaviour change campaigns or measure? How did they achieve scale and how were they evaluated?

This question is intentionally left blank.

25. Would you like to see cyber security features prioritised in products and services?

Yes, the GNGB believes this would assist in creating awareness and mitigating risks.

26. Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?

The Superannuation Transaction Network is a great resource that could be leveraged to improve the cyber security and reliance of all Australian businesses.

- The STN currently connects all Australian businesses with Superannuation funds and the ATO. 694,000 separate employer ABNs have been reported through the STN since 1 July 2018.
- The STN has a relatively small number of access points that are well organized, with a central point of contact and coordination, being the GNGB. The ability to roll out changes and initiatives is an established process (e.g. GNGB and its Gateway Operator Members of which there are 9).

- The STN has the potential ability to directly influence the cyber protection practices of all Australian businesses connecting to it.

GNGB
GATEWAY NETWORK GOVERNANCE BODY

Gateway Network Governance Body Overview

MICHELLE BOWER, EXECUTIVE OFFICER, NOVEMBER 2019

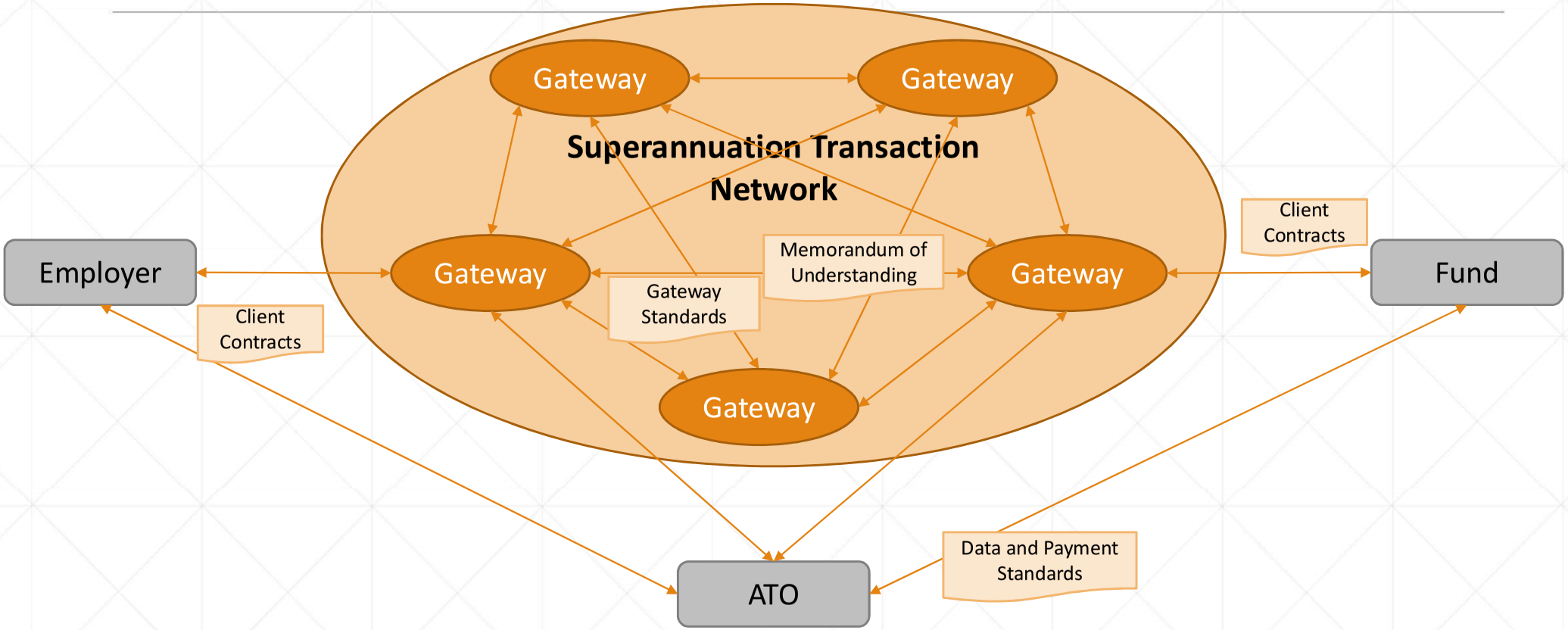
APPENDIX B

What is the GNGB?

The Gateway Network Governance Body Ltd (GNGB) has been established as an industry owned, not-for-profit organization, whose purpose is to manage **the integrity of the Superannuation Transaction Network (STN).** GNGB was established to implement the governance of the STN in 2016 at which time, the governance role was migrated to industry from the ATO. GNGB fulfil this purpose by:

- **monitoring compliance** with the Gateway Standards with reference to the SuperStream Data and Payment Standards, information security requirements and other agreed business and technology service levels
- undertaking initiatives or taking steps to promote the **efficiency and effectiveness** of the STN, continuous improvement and risk management
- managing **new entrants** and exits to the network
- and **engaging with key stakeholders** in Government and industry.

GNGB Scope – Governance of the Superannuation Transaction Network (STN)



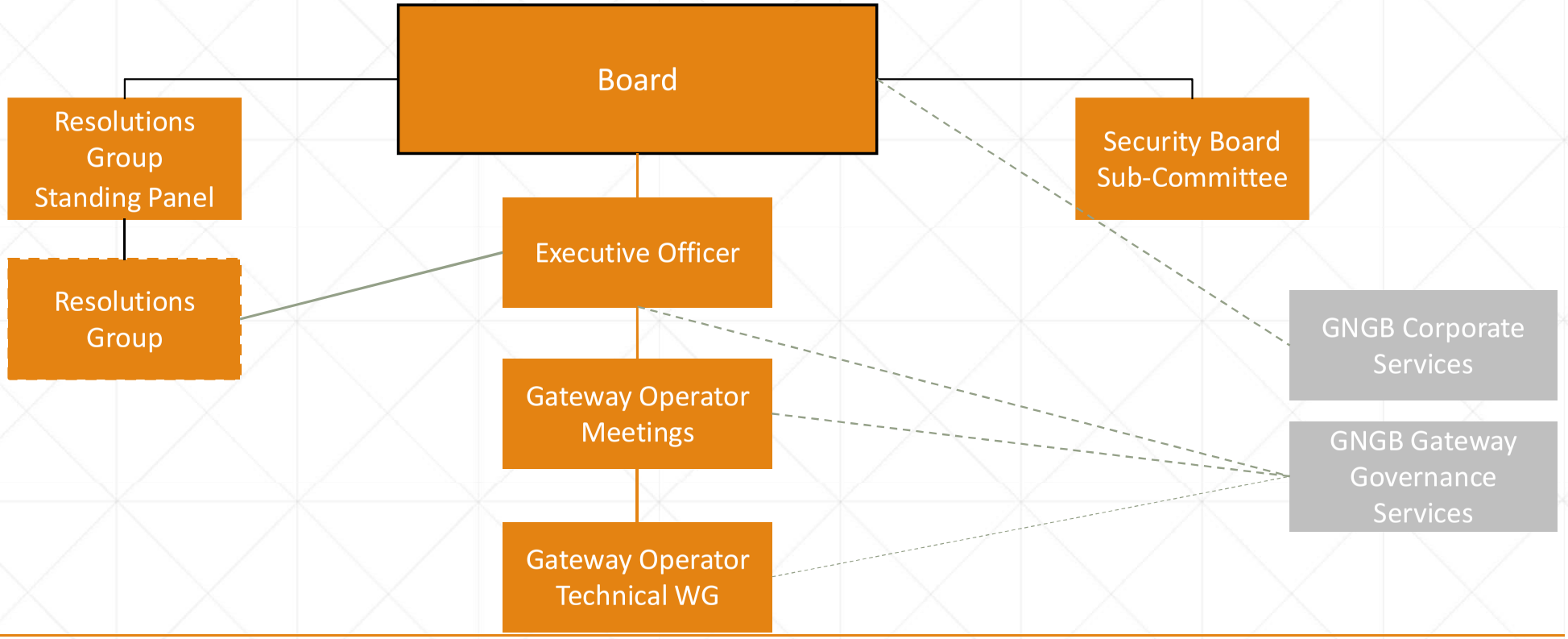
GNGB
GATEWAY NETWORK GOVERNANCE BODY

GNGB Key Governance Artefacts

The GNGB has the following key artefacts to support the governance of the STN

- Memorandum of Understanding for Participants in the STN
  - Provides the agreement between the GNGB and the Gateway Operators, the “rules of operating”
  - Includes:
    - Gateway Standards
    - STN Information Security Requirements
- GNGB Constitution

GNGB Structure



GNGB Board Composition

In line with the GNGB Constitution, GNGB Board is made up of an agreed representation of STN stakeholders inclusive of Superannuation Funds, Employer representation, software providers, and the Gateway Operators , plus an Independent Chair. The current GNGB Board comprises of the following Directors:

- Independent Chair – Jan McClelland AM
- Co-Sponsor (Funds) – Hans van Daatselaar (ASFA)
- Co-Sponsor (Funds) – Melissa Birks (AIST)
- Co-Sponsor (Funds) – Jane McNamara (FSC)
- Co-Sponsor (Software) – David Field (ABSIA)
- Employer Sector – David Humphrey (appointed by ACCI)
- Gateway – Ian Gibson (Superchoice)
- Gateway – Michael Ross (Message Exchange)
- Gateway – Mark Hudson (SunSuper)

GNGB
GATEWAY NETWORK GOVERNANCE BODY

Gateway Operators

Gateway Operators are those gateways who have signed the Memorandum of Understanding with the GNGB. This is the agreement between the GNGB and Gateway Operators that establishes the Gateway Standards, and provides the “rules of engagement” with the STN.

The current Gateway Operators are:

ClickSuper	Ozedi
GBST	SunSuper (Precision)
IRESS	Superchoice
MessageXchange	Westpac (QuickSuper)
Oban	

https://www.gngb.com.au/

Appendix C – Call for Views - Cyber Strategy 2020 Submission

GNGB
GATEWAY NETWORK GOVERNANCE BODY

Gateway Network Governance Body Cyber Security Incident Response Planning
First Annual Report, August 2019

SARAH O'BRIEN, EXECUTIVE OFFICER

GNGB
GATEWAY NETWORK GOVERNANCE BODY

The GNGB, Cyber-Security and Superannuation

The Gateway Network Governance Body Limited (GNGB) is the self-regulatory body for the Superannuation Transaction Network (STN), the network used to send and receive superannuation transaction messages between Gateway Operators, on behalf of employers and superannuation funds.

Established in 2016 by the superannuation industry, gateway operators and software providers, it manages the integrity, security and effectiveness of the STN through a Memorandum of Understanding made with Gateway Operators in the superannuation industry.

As the governance body for the central network through which over 9 million superannuation data contribution and rollover transactions are routed every month, managed by 9 Gateway Operators, the GNGB takes very seriously its role in managing the security of that network, and has therefore established a GNGB Security Committee, focused on advising the GNGB Board on information and cyber-security matters affecting the network and provides a focal point for data security and cyber activities impacting the STN. The Committee has developed a range of artefacts and activities focused on information and data security.

GNGB
GATEWAY NETWORK GOVERNANCE BODY

The GNGB, Cyber-Security and Superannuation

The security of the STN is a vital part of the security of superannuation data and information generally. The network carries personal taxpayer data, and as such is an identified target for cyber-security threats. Superannuation funds, employers and fund members expect the network to protect the data it carries, and the recently updated APRA CPS 234 makes clear that the requirements of the Prudential Standard extend to third parties who manage information assets for APRA-regulated entities. This makes this activity a vital part of the security of the employer/superannuation environment as a whole.

It is important to note, however, that the scope of the governance responsibilities of the GNGB do not extend to the exchange of data and information between Gateway Operators and their clients, and therefore the extent to which the activities managed by GNGB protect the superannuation industry is limited.

The GNGB is keen to engage further with industry on further measures that could be taken to protect the security of the full data interactions across the superannuation landscape.

GNGB
GATEWAY NETWORK GOVERNANCE BODY

The GNGB and Cyber-Security Activities

The GNGB aims to:

- support Gateway Operators and the superannuation industry to be aware of cyber-security issues
- have a range of practical technology and process controls to address cyber risk to the network
- foster open discussions about cyber threats and solutions

The GNGB achieves these objectives through:

- agreed Superannuation Transaction Network Information Security Requirements (STN ISR) that Gateway Operators adhere to, that represent industry best practice
- annual verification of compliance with the STN ISR through an annual independent audit
- ongoing discussion of cyber risk matters at Board and operational forums
- a Cyber-Incident Response Plan, providing a framework and guidance for the GNGB and Gateway Operators to respond in the event of an incident
- annual test of the Cyber-Incident Response Plan through a walkthrough exercise, testing a range of scenarios

STN Cyber-Incident Response Plan

Over January to June 2019, Deloitte were engaged by the GNGB Board to develop a Cyber-Incident Response Plan, which provides the GNGB and Gateway Operators with a plan to manage a network-wide response to a range of cyber-security incidents.

The plan is designed to supplement Gateway Operator's own Incident Response Plans, by providing a framework to establish roles and responsibilities, manage communications and network decision making, and support participants in managing an incident, identify the causes of an incident, and recover to full operation.

The Plan was approved by the Board on 15 July 2019, and now forms part of the range of artefacts available to the GNGB to manage the security of the STN.

STN Cyber-Incident Response Exercise

On 6 June 2019, Deloitte facilitated a a Cyber-Incident Response Exercise ("Exercise") for the GNGB and Gateway Operators to:

- Test the Cyber-Incident Response Plan ("Plan")
- Ensure all participants are familiar with the plan and have the opportunity to experience it in a scenario exercise environment
- Provide opportunity to improve and refine the Plan
- Provide opportunity for stakeholders to participate, observe and provide feedback on the Plan and the Exercise

The Exercise was to run desktop scenarios, and designed to test the actions taken by and the interactions between Gateway Operators, the GNGB and the ATO. Other stakeholders were invited to observe.

The Exercise did not extend to interactions involving superannuation funds, employers or other stakeholders, except to occasionally observe that they may need to be informed or involved at certain points in the Exercise scenarios.

Cyber Security Incident Response Exercise Overview

GNGB
GATEWAY NETWORK GOVERNANCE BODY

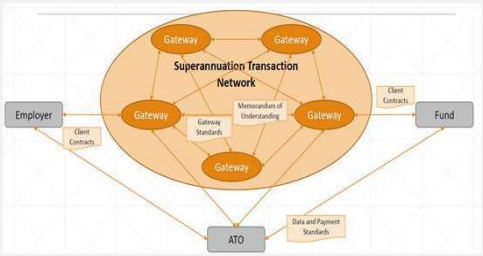
Objectives:

- Current understanding of the draft Cyber Incident Response Plan
- Internal and external communication across the STN
- Decision making and coordination between Gateway Operator and GNGB
- Differentiate between the business continuity and incident response plan

Exercise Scope:

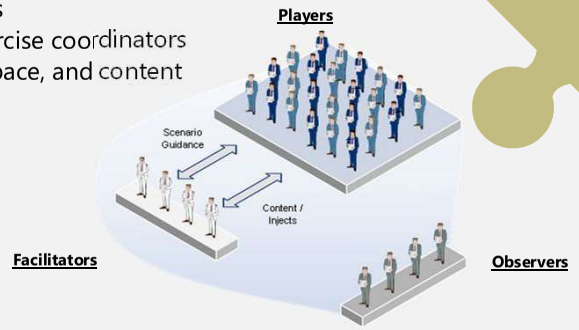
Players, in the exercise, included representatives from all the gateway operators, GNGB and ATO. The exercise also had a number of observers from GNGB, gateway operators, APRA and ATO.

The facilitators and observers made several observations during the exercise which we have summarized in this report.



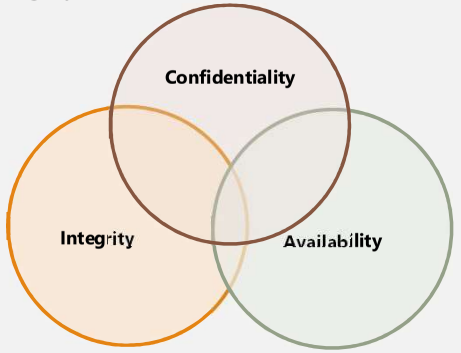
Participants:

- **Players:** Simulation exercise players that respond to scenario injects
- **Observers:** Stakeholders that observe player's decision making and actions
- **Facilitators:** Simulation exercise coordinators that manage the direction, pace, and content of the exercise



Scenarios Used:

The Deloitte team conducted a simulation exercise using three different cyber attack scenarios aimed at the information security triad i.e., confidentiality, availability and integrity.



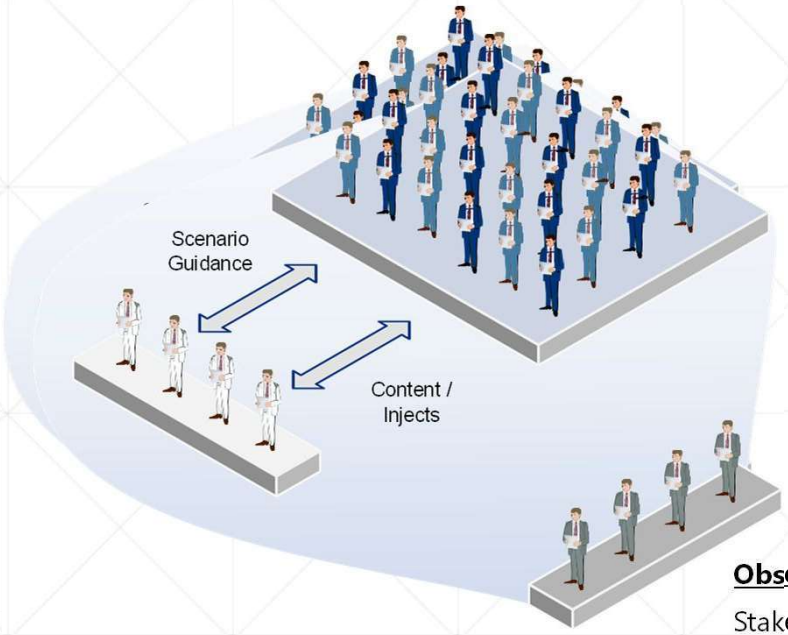
Participants

Three sets of stakeholders who participated in the exercise

Players

Simulation exercise players that respond to scenario injects

GNGB, Gateway Operators, ATO Services Representative



Facilitators

Simulation exercise coordinators that manage the direction, pace, and content of the exercise

Deloitte

Observers

Stakeholders that observe player's decision making and actions

Co-Sponsors, ATO, APRA

GNGB
GATEWAY NETWORK GOVERNANCE BODY

Exercise Scenarios

Scenarios were selected to test a range of possible events and responses. Three scenarios were completed:

1. A ransomware attack affecting availability, commencing with one Gateway Operator, then spreading to further Gateways.
2. A social media report of a data breach involving superannuation and taxation related personal information, reported by more than one Gateway Operator, with an associated increase in rollover activity to Self-Managed Superannuation Funds.
3. A data integrity issue identified with TFN mismatches, followed by a Gateway Operator identifying a “data leak” from internal systems. Investigation identifies spear phishing emails.

GNGB
GATEWAY NETWORK GOVERNANCE BODY

Observations

- The Exercise clearly demonstrated that the GNGB has a vital and significant role in supporting the STN, ATO and the wider superannuation environment in managing activity and communications across industry participants. There is an ongoing need for the GNGB and its responsibilities to share information, coordinate responses and communications, and provide support to the industry in planning for and managing incidents.
- All participants were highly engaged and responsive in the operation of the Exercise.
- The players were open in their interactions, and worked together to identify issues, and determine possible resolutions.
- The Exercise provided an effective test of the Plan, and identified areas for improvement
- The Exercise provided some areas for improvement in the STN and GNGB's response to a cyber-security incident, which are currently being addressed by the GNGB

GNGB
GATEWAY NETWORK GOVERNANCE BODY

Next steps

The GNGB continues to develop processes and activities focused on improving the cyber-resilience of the Superannuation Transaction Network, including:

- Updating the Cyber Incident Response Plan with recommendations made from the Cyber Incident Response Exercise
- Repeat of Cyber Incident Response Exercise annually to build familiarity and confidence, and provide continuous improvement opportunity
- Independent review of the STN ISR to ensure it is consistent with cyber security best practice
- Development of a quarterly discussion group focussed on learning from known incidents and threats, and providing opportunity to continuously improve the security of the STN

GNGB
GATEWAY NETWORK GOVERNANCE BODY

What next?

This activity addresses part of the cyber-security issues that face employers and superannuation funds. Further work is needed across the industry to build the cyber-resilience of all systems and interactions to ensure that fund member data is protected.

The GNGB invites any expressions of interest in being involved in the next steps to expand the work that we have begun.

Questions and contacts

Michelle Bower, Executive Officer

[redacted]

gngb.com.au