Gateway Network Governance Body
contactus@gngb.com.au
www.gngb.com.au
27 February 2024

Australian Government
Department of Home Affairs
Via Consultation Web form
cisgcomms@homeaffairs.gov.au

RE: Gateway Network Governance Body Ltd's (GNGB's) submission on Cyber Security Legislative Reforms: Consultation on proposed new cyber security legislation and on changes to the Security of Critical Infrastructure Act 2018

Thank you for the opportunity to provide feedback into the proposed changes to implement the government's vision and 2030 cyber security strategy, as well as input into proposed changes on the SOCI Act 2018.

GNGB is the industry owned governance body responsible for the security, integrity and availability of the Superannuation Transaction Network (STN), the data infrastructure that transmits superannuation transactions such as rollovers and contributions between superannuation fund trustees and employers. Superannuation fund trustees and employers rely on the STN to enable their legislative superannuation obligations. The STN comprises of 9 Gateway Operators who validate, route and transmit superannuation transactions, in line with the Superannuation Data and Payments Standards.

Since 2016, GNGB's role as a governance body has included the implementation of a risk management framework and information security obligations across Gateway Operators within the environment, promoting awareness and fostering collaboration in dealing with threats to the resilience of the STN. It is in this context, that GNGB provides the following submission to the department of Home Affairs, for consideration. This submission has been developed in discussions with Gateway Operator organisations.

Summary

GNGB is supportive of measures that promote collaboration of industry and government to improve situational awareness and availability of actionable intelligence for all organisations to use, in the protection against cyber threats. Government is well placed to understand the holistic threat landscape and therefore lead the way in providing information organisations can use to protect themselves. GNGB supports reporting requirements that enhance the government's view of the threat landscape, however there is limited value in applying penalties for non-compliance to reporting or information sharing deficiencies and the department of Home Affairs should have discretionary powers to enable flexibility in their application.

With regard to changes to SOCI Act 2018, GNGB is supportive of additional powers for the CISC in relation to consequence management and review and remedy of critical assets risk management processes however, appropriate safeguards are essential to ensure the best allocation of resources for organisations in managing their individual risks. In addition, it is not clear how the department will identify "deficiencies" in relation to risk management programs. A clear transparent and consistent approach is required to ensure there are no surprises for critical infrastructure asset owners and operators. GNGB supports changes to the definition of Protected Information to ensure

better sharing of intelligence to enhance situational response to threats, however GNGB also recommends renaming the information set to be more indicative of what is to be protected. We suggest “CI Data” should be considered as a classification to avoid confusion with other frameworks already in place.

Detailed GNGB Response

Measure 2: Mandatory Ransomware reporting for all entities greater than $10M turnover

Scope and timeframes for reporting

GNGB proposes an alignment of proposed Part 1 reporting to the existing mechanism required for Critical Infrastructure (CI) owners and operators, embedding consistency across all organisations experiencing a ransomware attack. The timing of reporting requirements should not interfere with the organisations’ ability to respond effectively to the attack, which should be prioritised. For this reason, the timeframe for non CI organisations may be longer, post identification of the impact, however GNGB supports consistency of approach to existing regulations. The objective of the data collection needs to be considered and as the purpose here is to collect actionable information on the threat itself, this may be up to 14 days.

Once a ransom is paid (Part 2 reporting), it makes sense for the information relating to payment recipient and instructions provided to the payee, to be reported. This information can assist in identifying the perpetrator and contribute to law enforcement investigations of the criminals.

With the stated objective of “developing our national threat picture”, GNGB does not support the exclusion of businesses under $10M turnover per year. Reporting known information about the attack via a webform should not be overly burdensome to small or medium sized organisations and will contribute to the overall threat picture. Often vulnerabilities are targeted at those with less resources directed to their cyber defences and reporting by all types of organisations will assist to identify trends or systemic weaknesses, for which strategies can be applied.

Incentives for Reporting

GNGB supports the No Fault/No Liability protection principle being applied to ransomware reporting as this incentivises the sharing of actionable and specific intelligence that can be operationalised by other organisations and government.

Sharing of threat information with organisations should act as an incentive to comply with reporting requirements. As an output of the reporting mechanism, it would be beneficial for organisations to receive practical and actionable information in relation to:

- vulnerability exploited or point of compromise
- indicators of compromise
- tools, techniques and tactics used by the perpetrators
- attribution to a particular group or individual to enable organisations to understand the changing or shared tactics of perpetrators

The closer to real time events that sharing of the above information occurs, the better to be able to operationalise the information for proactive cyber protections. GNGB considers a monthly bulletin detailing all relevant incidents may be appropriate. GNGB recommends the use of existing communications mechanisms when sharing this type of information such as the TISN or the ACSC partnership program channels.

Measure 3: Limited use obligation on ASD and NCSC to encourage engagement

A clear limited use obligation is an incentive to engage on cyber issues both proactively, and during the aftermath of an incident. GNGB supports limiting the use of reported information for prescribed security purposes, excluding regulatory compliance purposes, however it should include:

- use in the investigation and apprehension of cyber criminals by law enforcement agencies
- use by intelligence agencies for protection of the national interests
- use in the support of a response to impacted entities where requested
- use in education programs and guidelines developed by government, such as the Essential 8

Restrictions on Sharing with government agencies

What is of value to information receivers is actionable and specific intelligence on the indicators of compromise and the behaviour or tactics and techniques used by the perpetrator(s). This allows peer organisations to take proactive steps to protect their own environments from the same or similar threats. With this objective in mind, information regarding the organisation under attack is not required (unless an organisation is directly within the sphere of impact at which point we would expect notification to be within the organisation's incident response protocols). Sharing of the threat actor activity, root cause and steps taken by the attacker are of the most helpful and organisational identifiers are unnecessary.

Incentives for industry to engage during a cyber incident includes the building of trust in the partnership between industry and government. Industry needs to see value in the outcomes – i.e. where actionable and timely intelligence is shared, organisations big and small will see the value in sharing information when something happens to them.

Measure 4: A cyber incident review Board

GNGB supports the concept of a cyber incident review board for its ability to shed light on weaknesses within the Australian ecosystem, and the sharing of lessons learned to collectively uplift cyber defences over time.

GNGB considers that review of cyber incidents by a CIRB should be determined on a risk basis. Characteristics such as the impact on citizens, number of services impacted by lack of availability, degree of personal data compromised should factor into decisions on the potential benefits of a CIRB review. It would also be useful for the CIRB to review incidents that indicate unusual, or a change in, attacker behaviour or the use of new technology or tools by an adversary. Learnings from such a review would likely have a significant, positive impact on the broader ecosystem.

CIRB should be staffed by Cyber experts, across a diverse range of capabilities and backgrounds. Independence is key to ensure good governance and GNGB considers a core group of the board to maintain independence and good governance principles, to be matched with subject matter experts from a panel of approved personnel, to be selected based on the incident type. Conflict of interest will need to be managed closely by the standing board members and strict criteria about connection to the incident should be adhered to.

Any published outcomes of the CIRB's review should be done so on an anonymous basis, so as not to disclose confidential information of the organisation/s under review.

GNGB acknowledges that there will be times where information is already in the public domain (e.g. where the incident had a significant impact on the general public) at which point, anonymity is of no value. In a no fault process however, the impacted organisation should be made aware by the CIRB of any release of public information well before this occurs, to enable management and preparation

of their stakeholders (a no surprises environment). The CIRB must work in partnership with the organisation(s) under review. This no fault approach will incentivise organisations to provide information. Effective reviews can only be undertaken when all the facts of the matter are known to the CIRB.

Measure 5. Changes to definitions to include data storage assets as in scope of the SOCI act, when they include business critical data but are not part of the Critical Asset itself.

It is GNGB's view, that the definition of the assets making up the Critical Infrastructure data sector has always been ambiguous. GNGB recommends further clarification of this definition, perhaps supported by some case studies, to accompany the tweaks to include data storage assets explicitly in scope.

The changes proposed to the definition of data storage assets in scope of the SOCI Act does not appear to have an impact on Gateway Operators as data storage applications and infrastructure are already considered part of the asset. In addition, segregation of the Gateway (asset) from corporate networks is a requirement under the Superannuation Transaction Network Information Security Requirements (STN ISR).

Measure 6. Consequence management powers

GNGB supports the additional powers to manage consequences of an incident in relation to a Critical Infrastructure asset, provided the safeguards outlined are adhered to. GNGB considers the parallel ministerial powers to direct action in response to an incident and that they have yet to be used, indicating a high threshold required to invoke those powers.

An example of where this may be of use is in the sharing (via safe and secure means) of Personally Identifiable Information (PII) that has been stolen, with the objective of alerting or protecting the individuals whose data has been exposed. This would be in breach of our interpretation of privacy laws however ministerial directions to share with government or other organisations, would potentially assist in the implementation of protections for those individuals.

Measure 7. Protected information powers

According to the CISC, the department has experienced limitations during incident management due to ambiguity on the ability to share CI information. The proposal is to tweak the definition within the Act to enable threat sharing or information sharing to occur without stepping on restrictions within the Act.

Protected information under SOCI is different to the "protected" categorisation of data that is used within the STN. The STN has classified data as Protected based on the Protective Security Policy Framework (PSPF)*[1] published by the ACSC. GNGB recommends consideration of a different term to indicate information required to be kept confidential under the SOCI Act, to avoid confusion.

[1] Protected Information - High Business Impact. Compromise of information confidentiality is expected to cause: Damage to the national interest, organisations or individuals

At GNGB, we set the scope for Gateway Operators under our governance to protect STN Data, which is then defined. Could “CI Data” be a defined term under the Act to explicitly refer to the objectives of the information protections with respect to data requiring safeguards under the Act?

GNGB supports a harms based approach for entities when considering whether to disclose information but also considers the harms that may be caused by not sharing that information at a crucial point in response, recovery or consequence management of an incident. Guidance will be required for entities to operationalise a harms based approach, to ensure consistency of application.

Measure 8. Review and Remedy Powers

The proposal under this measure outlines where the CISC identifies deficiencies in the risk management programs (RMP’s) of CI assets. This proposal introduces a power to direct organisations to uplift risk management programs. Entities are currently not asked to submit their RMP’s (as per existing drafting) but may be asked to provide the RMP under the existing information gathering powers where non-compliance is identified. It is not clear how non-compliance will be identified except in the case of an actual incident that indicates a weakness or vulnerability. GNGB requests clarification of the trigger for a request for further information. GNGB is supportive of a continued principles based approach to the risk management program which by its nature indicates CI asset owners and operators are best placed to identify and mitigate risks in their environment.

GNGB would welcome an opportunity to discuss any of the above comments or issues raised. Thank you for your consideration of GNGB’s submission.

Kind Regards

Michelle Bower
CEO
Gateway Network Governance Body Ltd

Jan McClelland AM
Chair
Gateway Network Governance Body Ltd