macquarie
TECHNOLOGY GROUP

Submission to Department of Home Affairs Consultation Paper on the Australian Cyber Security Strategy Legislative Reforms 2023-2030

1 March 2024

Introduction

1.1 Macquarie Technology Group Ltd (**Macquarie**) welcomes this opportunity to contribute to the Department of Home Affairs Consultation Paper on the Australian Cyber Security Strategy Legislative Reforms 2023-2030 ('**the Paper**').

1.2 Macquarie's interest in the Australian Cyber Security Strategy 2023-30 touches many areas highlighted in the Paper and we have done our best to respond to each question therein. Our submission is focused on the Government's goal for Australia to be the most cyber secure nation in the world by 2030 and, where possible, we have detailed practical solutions we believe are critical to achieving this goal.

1.3 Macquarie is subject to the Security of Critical Infrastructure (**SOCI**) regulatory regime in multiple capacities: as a licensed carrier under the *Telecommunications Act 1997* (Cth), a cloud service provider, and the owner and operator of Australian data centres which store and process the data of Commonwealth and State/Territory governments, as well as critical infrastructure providers and corporate customers.

1.4 Macquarie's data centres and cloud services are "certified strategic" under the Commonwealth Government's Hosting Certification Framework (**HCF**). Macquarie is the only company to achieve certification under the HCF for both data centre and cloud services. Macquarie's data centres are also declared Systems of National Significance (**SONS**).

1.5 Through internet/ perimeter defence services, cyber security and secure operations services, Macquarie provides cyber security and secure data storage/processing to approximately 42% of the Commonwealth government (as measured by staff head count).

1.6 For many years Macquarie has been investing in and advocating the goal for Australia to be a leading cyber secure nation. The strategic decision to locate and construct our data centres in Australia and to achieve HCF certification and SoNs recognition are clear evidence of our ongoing and longstanding commitment to supporting a robust cyber security posture for Australia.

1.7 We also wish to acknowledge that cyber security cannot be considered in isolation where regulation is concerned. We recognise the importance of other key Government reforms. In summary, Macquarie is an important stakeholder in the development of the Australian Cyber Security Strategy 2023-30 and we hope the Department of Home Affairs finds our input both insightful and helpful.

1. **Part 1**

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices

1. **Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?**
2. **Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?**
3. **What alternative standard, if any, should the Government consider?**
4. **Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?**
5. **What types of smart devices should not be covered by a mandatory cyber security standard?**
6. **What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?**
7. **Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for IoT devices?**

1. Macquarie acknowledges that consumer-grade IOT devices pose risks to cyber security and can used by cyber threat actors to target consumers and result in cyber-attacks. Macquarie also agrees with the general principle that IOT cyber standards should subject to a legislated mandatory standard. The Paper clearly articulates some of the problems with the adoption of voluntary standards (particularly in regards to the cost (and the nature of low cost IOT devices) and low levels of adoption) in an area where the consequences can be far reaching and have a waterfall effect on consumers and industry alike.

   Indeed, it is foreseeable to Macquarie that a customer with a passphrase used in a consumer IOT device, which was also used in a cyber or cloud product hosted by Macquarie, "*credential stuffing*" (noting that while this should not occur human nature indicates that it does and will continue to occur) which was hacked, could have devastating consequences for our customers, including other organisations that are subject to SOCI.

2. While Macquarie does not propose to opine on which specific standards should be used in regulating IOT devices, Macquarie does agree with the general principle that the standard applied should be internationally accepted to ensure that Australia remains in step with the international market, minimising regulatory burden for manufacturers and the assisting the transferability of products.

3. Again, while not expressing a specific opinion on the applicable timeframe, but noting that consumers (and industry) will continue to face risks as more products are developed and sold prior to commencement of the standard, Macquarie agrees there should be an appropriate time period to enable industry to adjust to any new requirements. A 12 month transition period (as seen in the SOCI Act) does seem to be at the higher end of the scale (particularly after legislation is passed and prior to commencement of any new obligations). While a 12 month transition period was applied to SOCI, Macquarie would submit that it is significantly more cumbersome to ensure cyber standards for critical infrastructure and repeats its comments around cyber concerns for IOT products at 1 above.

4. The Paper asks in Part 1 that Macquarie, as an input to critical infrastructure supply chains, should be responsible for complying with a proposed mandatory cyber security standard. Macquarie agrees that it appears sensible to take a similar approach to consumer product safety (i.e.. vendors, suppliers, importers and manufacturers all complying with the standard). However, Macquarie also notes the importance of ensuring that the infrastructure on which these devices sit also fall within the ambit of SOCI and therefore are not another hole or exception in the cyber security ecosystem. We discuss this in detail below. Put simply it is

obvious to Macquarie that if the IOT product had data stored on a telecommunications asset data storage system, it is unclear whether the telecommunications asset would be subject to SOCI as part of their existing risk management obligations. In the interests of strengthening Australia's cyber security posture, this needs resolving. Effectively, a 'security strong' IOT device could be sitting on a 'security weak' telecommunications asset.

5. With respect to the question "*What types of smart devices should not be covered by a mandatory cyber security standard*" Macquarie does note that some parts of industry have expressed concerns around smart telephone devices being subject to these standards. In relation to this perceived concern, Macquarie repeats its comments above, that in order to close the gaps in our current legislative and regulatory framework for cyber security (an aim of the Paper), we need a fulsome legislative response rather than have specific devices and infrastructure not subject to the regimes.

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses

7. **What mandatory information, if any, should be reported if an entity has been subject to a ransomware or cyber extortion incident?**
8. **What additional mandatory information should be reported if a payment is made?**
9. **What is the appropriate scope of a ransomware reporting obligation to increase visibility of ransomware and cyber extortion threats, whilst minimising the regulatory burden on entities with less capacity to fulfil these obligations?**
10. **Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?**
11. **What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?**
12. **To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident?**
13. **How can the Government ensure that no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?**
14. **What is an appropriate enforcement mechanism for a ransomware reporting obligation?**
15. **What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, and with whom?**

6. Macquarie agrees with the Paper's proposition that limited visibility of the ransomware and cyber extortion threat restricts the capacity of the government and private sector to help Australian organisations prepare for, and respond to, these incidents. We agree that timely reporting of ransomware and cyber extortion incidents would accelerate remediation and responsiveness.

7. We agree that corporates should be mandated to provide Information regarding a ransomware attack for the reasons articulated in the Paper. Such information sharing is vital for Government to enhance our national threat picture and notes that Macquarie already voluntarily provides its customers, including Federal Government agencies, a "*Weekly Threat Report*" for these reasons. The information included in this report includes, for example, the frequency and the country of origin of threats blocked by Macquarie. The Report dated week Ending 18th February 2024 noted "*Macquarie Government's Cyber Threat Intelligence (CTI) team actively reviews SIGNET telemetry to identify notable events and conduct intelligence-led threat hunts. These are the statistics from the past week: In the last 7 days Macquarie Government has blocked 11.2 billion events…shows the top 10 countries of origin from 9.7 million blocked IPS events*." A copy of this report is attached and marked "Appendix A".

8. The Paper's list of proposed information to be reported resonates with Macquarie and its cyber engineers including:

• when the incident occurred, and when the entity became aware of the incident;
• what variant of ransomware was used (if relevant);
• what vulnerabilities in the entity's system were exploited by the attack (if known);
• what assets and data were affected by the incident;
• what quantum of payment has been demanded by the ransomware actor or cybercriminal, and what method of payment has been demanded;
• the nature and timing of any communications between the entity and the ransomware actor or cybercriminal; and
• the impact of the incident, including impacts on the entity's infrastructure and customers.

9. Macquarie is however concerned about limiting this reporting obligation to businesses of a certain size or threshold. This concern is twofold. Firstly, Macquarie repeats it general concerns regarding exceptions to cyber security standards. In order to close the gaps in our current legislative and regulatory framework for cyber security (an aim of the Paper), we need a fulsome legislative response rather than have specific businesses not subject to the regimes. Indeed, it is foreseeable that some large corporates may seek to structure their businesses so that the reporting entity does not meet the requisite size set by the Government as a way to avoid this reporting regime, which again would make the aims of the Government redundant. Our second concern, and one which we understand is shared more broadly with members of industry is that by limiting disclosure obligations to entities of a certain size may make entities which fall below that threshold more of a target for cyber criminals.

10. Macquarie submits that the way to assist small businesses and the perception that they may not be in a position to absorb the additional regulatory burden imposed by a new reporting obligation is to make the threat sharing as simple as possible. Macquarie has heard from members of industry that "*a telecommunications entity had to report to 28 areas of governments after a data breach.*" While Macquarie does not share that experience, we do experience significant confusion around reporting, and support the idea that further education in this area (even to large telecommunications companies) is needed. We also note that applying the Government's "Single Reporting Portal" (Single Reporting Portal | Cyber.gov.au) a telecommunications entity that listed as critical infrastructure would have at least five mandatory reporting obligations and potentially more if they meet any other requirements such as ASX listing, APRA regulation, licenses and so forth. It is clear that reporting obligations are cumbersome and could be streamlined. Indeed, this was noted by the Government in its very recent paper 'HWL Ebsworth Cyber Security Incident, Lessons Learned Review'. We discuss ways to assist in this regard below regarding a **Cyber Alliance Board**.

11. Macquarie also notes that threat sharing by companies, even small businesses, with reasonable cyber security protections is largely automated. In the circumstances, there should not be significant regulatory burdens for small business in complying with these reporting regimes. In fact, the proposed regime may encourage adoption of simple and price effective cyber security protections, which would have positive impacts for Australia's broader cyber security posture.

12. Macquarie also notes in this regard that the proposal that a report is to be made within 72 hours of an incident occurring, is reasonable. Macquarie's cyber engineers suggest that a lot of the information captured is largely automated and that such a timeframe would ensure there is less focus on having legal teams review and 'guide the pen' on the sharing of information. It is commonly known that a focus on legal regulatory approaches has narrowed what industry shares with government, including threat intelligence, which is pushed to legal compliance teams before dissemination. Macquarie's opinion is that a 72-hour timeframe would reduce this culture of legal review verse industry threat sharing and the positive information flow that can follow.

13. Macquarie broadly supports the no-fault and no-liability principles suggested in the Paper. Macquarie shares the Government's view that greater understanding of the threats we are facing will assist the Government and industry to adapt to the rapidly evolving cyber security landscape. However, Macquarie does have concerns about what these principles might look like in practice and respectfully submits that the paper does not provide the requisite level of detail.

14. One such concern is how information shared with the Government might be used in a civil dispute, such as a class action. The time a company became aware of a cyber breach is a fact that could be used by a civil litigant, for example, in an argument to prove that the company and its directors did not act in the best interests of its shareholders. It is apparent to Macquarie that information shared could invariably be subject to a discovery action and such disclosure may expose corporate, and its Directors & Officers, to liability. Macquarie notes similar issues around indemnification were raised (and not resolved) in the US with the *Cybersecurity Information Sharing Act*.

15. Macquarie has heard from the Department of Home Affairs that a solution to this might be attaching legal privilege to the disclosure or limited FOI protections. Macquarie would like to understand precisely what is proposed in this regard to overcome this difficult conundrum of information sharing and potential exposure. At this stage, it is difficult to see how legal privilege could assist as well as balance the concerns at 13 above regarding 'legal review' and timeliness of information sharing and separately note that any legally privileged information or FOI requests would nonetheless be discoverable for the purposes of civil proceedings but simply marked "privileged". We would be interested in hearing more from the Office of Parliamentary Counsel or Department on any proposed wording.

16. The Paper also asks what types of anonymised information about ransomware incidents would be most helpful for industry to receive? Our cyber engineers have suggested that it would be helpful to receive (as frequently as possible):

    a. data on the number occurrences of the variant targeting Australian organisations and by what sector;
    b. details on mitigation steps taken of the exploited vulnerabilities; and
    c. known methods of reversing encryption (if known).

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

17. **What should be included in the 'prescribed cyber security purposes' for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?**
18. **What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?**
19. **What else can Government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?**

17. Macquarie broadly supports the Paper's proposed limited use obligation to encourage information sharing. We share the Paper's concerns around delays in entities providing technical information relevant to ongoing cyber security incidents, as discussed above. We also repeat our concern regarding legal team review and 'guide the pen' on the sharing of information and note that Macquarie voluntarily shares threat sharing information with its corporate and Government customers on a weekly basis.

18. We support the fact that the proposed 'limited use' obligation would restrict the **use** of cyber incident information, but not the **sharing** of this information. We consider that this strikes a

good balance between the importance of threat sharing and potential exposure, although we still have some concerns regarding civil exposure as discussed above at 15 and would welcome further consultation on this difficult subject.

19. The US CISA is a good precedent, but not without its limitations (regarding indemnity, again raised above). We can look to CISA Act for a precedent that provides a regime for the sharing of industry threat information with relevant federal agencies and also clarifies that information provided cannot be used to bring an enforcement action, while regulators continue to have access to their existing set of information gathering powers. We support this proposal. We also broadly support the definition of Cyber Security purposes on page 20 of the Paper.

20. The Paper asks what else the Government can do to promote and incentivise entities to share and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident. We strongly acknowledge the importance of this collaboration have considered the issue in detail and suggest that Government consider the establishment of a Cyber Alliance Board to assist this objective.

    Macquarie is in a unique position. It is a Critical Infrastructure provider, a SONS listed entity, certified under the HCF framework; as well as a telecommunications provider and provider of cyber security to a large number of Government customers. Subsequently, Macquarie is involved in a significant number of Government and industry-based consultation groups which span these areas. Nonetheless, and perhaps because of this, we consider that there is still a real need for a cyber-specific co-regulatory industry group. We participate in the SoNS Threat Intelligence Sharing Network (**TISN**), members of the Australian Telecommunications Security Reference Group (**ATSRG**) and attend numerous roundtable and industry consultations.

21. To best achieve outcomes while working together we suggest the Australian Government look to other co-regulatory approaches to support and encourage industry self-regulation as models for best practice. The Telco sector in specific, which is a related field (with technology, data and connectivity being at the core), provides a useful precedent for co-regulation.[1] The Telecommunications Bill Explanatory Memorandum 1996 details arrangements for the establishment of a codes of practice regime designed to provide a framework for industry self-regulation. This regime considers the possibility that industry consensus might not always be achievable, and safeguard provisions have been developed. It details that codes and standards are to reflect the legitimate needs and interests of all industry stakeholders and that consultation must occur with the industry (such as Communications Alliance (CA)) the public and representatives of consumer groups.

22. The co-regulatory model, or Cyber Alliance Board, could focus specifically on co-regulatory and legislative matters while keeping the existing TISN, industry and security discussions separate. For example, the current SOCI reviews the subject of this paper and those scheduled for 2025 would clearly benefit from a legislative guidance from key cyber industry stakeholders. In our view, the matters raised in this paper make the benefit of such The Cyber Alliance Board quite apparent, and we discuss this in the context of the Cyber Incident Review Board at 30 below. The Cyber Alliance Board would provide within the cyber sector, the opportunity for industry and regulators working together to devise rules and regulation which would invariably see members of industry "on-board".

---

[1] Other examples include: The Australian Association of National Advertisers (AANA). The AANA established a Code of Ethics and the Advertising Standards Bureau, which incorporates an independent Advertising Standards Board to hear complaints regarding advertising content. The *Broadcasting Services Act 1992* (Cth) also industry co established the Commercial Television Industry Code of Practice and the Commercial Radio Australia Code of Practice and Guidelines. Other examples include the various codes of conduct regulated by the ACCC: see Industry codes | ACCC.

23. CA could provide a useful precedent for the Cyber sector. CA provides a forum for the telco industry (and a number of cyber and digital platform representatives) to make contributions to policy development and oversee the development of consultative industry codes of practice such as under the Telco legislative regime. The cogent theory being that industry, and particularly, cooperative industry, is the best source of knowledge particularly in relation to how best to regulate and respond to industry. The cyber industry, and cyber threats, are accelerating at an unprecedented pace and an agile and flexible approach to regulation is essential. We submit that co-regulation would be the best approach to keep pace and respond to these challenges. A body with industry representatives such as CA including management with expertise and gravitas in the growing cyber space, could provide valuable real time insight for the Australian Government. We envisage a scenario where the Cyber Coordinator could Chair the Cyber Alliance Board to heighten this real time insight and cooperation.

24. We submit that this need in this space is clear in circumstances where in facing expanded cyber threats, such as generative AI, regulation need to be flexible. In Macquarie's experience, some of the industry consultation that it is exposed to is not flexible or nimble. The Government's paper 'HWL Ebsworth Cyber Security Incident, Lessons Learned Review' notes on a number of occasions the need for better coordination (some 27 times!) and the need to "*develop processes to support broader engagement with industry and enable other directly impacted industry entities to benefit from a coordinated response to an incidents*". We submit that Cyber Alliance board would provide this coordination and 'broader engagement with industry'.

25. Co-regulation could also provide insight into essential areas such as, accreditation and certifications, again supporting shield 5 of the strategy and professionalisation of the Cyber workforce. Indeed, the action plan refers to industry 38 times (across threat sharing, cyber crisis response and breaking the ransomware model) and industry co-regulation could assist achieve all of these outcomes. It is also very clear that there is confusion in relation to cyber reporting (see 10 above), and again we see benefit in a Cyber Alliance Board to provide coordination and guidance and how Government better structure reporting and educating industry around these matters.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board (CIRB)
20. What should be the purpose and scope of the proposed CIRB?
21. What limitations should be imposed on the CIRB to ensure that it does not interfere with law enforcement, national security, intelligence and regulatory activities?
22. How should the CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?
23. What factors would make a cyber incident worth reviewing by a CIRB?
24. Who should be a member of a CIRB? How should these members be appointed?
25. What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?
26. How should the Government manage issues of personnel security and conflicts of interest?
27. Who should chair a CIRB?
28. Who should be responsible for initiating reviews to be undertaken by a CIRB?
29. What powers should a CIRB be given to effectively perform its functions?
30. To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?
31. What enforcement mechanism(s) should apply if entities fail to comply with the information gathering powers of the CIRB?
32. What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?
33. What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?

26. Macquarie is broadly supportive of the concept of a CIRB and the principles of formation set out in the Paper. Macquarie agrees that the Government should co-design with industry a Cyber Incident Review Board to conduct no-fault incident reviews to improve our cyber security.

27. We agree that the Government needs a mechanism that can disseminate clear and concrete recommendations to strengthen cyber resilience. The United States' Cyber Safety Review Board (**CSRB**) is a potential model. However, we disagree that the Australian Transport Safety Bureau (**ATSB**) is a precedent that should be followed. The ATSB was formed on 1 July 1999 and it investigates transport safety matters. This is a very established area with known and recognised risks and solutions which have been drawn from decades of research and data. Cyber is far less known. It is evolving every year. The cyber industry, and cyber threats, are accelerating at an unprecedented pace and an agile and flexible approach to regulation is essential.

28. For these reasons, adopting an ATSB type model should not be the solution. We again repeat the need for a Cyber Alliance type body to which the proposed CIRB would liaise and co-regulate. While we acknowledge the need for independence of the CIRB and the Government should directly appoint the Chair and Members of the CIRB and 'sign off" on when a review is initiated, it is clear that the Cyber Alliance body would provide helpful guidance on matters such as when a review should be initiated, what should be the scope of the review and that the Cyber Alliance body and Government should work together to co-regulate the proposed CIRB. We consider there would be benefit to having a member/s of the Cyber Alliance Board also sit on the CIRB.

29. More broadly, the constitution or similar of the CIRB should dictate that the findings and collection powers are governed by limited use and no fault principles. As mentioned at various points in this submission, it is clear that threat sharing and lessons learned need to be consultative rather than punitive.

30. The Paper asks, "*what factors would make a cyber incident worth reviewing by a CIRB*?". Indeed, this is a question that internally we would discuss with a cyber engineer given the

quickly changing landscape. In the same circumstances, we submit that it would be useful for the CIRB to have industry representatives from the Cyber Alliance Board to consult. However, at this stage, we consider: *Scale, Impact, loss, Notifiable Data Breaches, Involving SoNS or critical infrastructure and Use of Zero Day exploit* as matters which could trigger a review.

Part 2: Amendments to the Security of Critical Infrastructure Act 2018
How are you currently managing risks to your corporate networks and systems holding business critical data?
35. How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?
36. What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?

31. The Paper accurately suggests "*recent incidents impacting critical infrastructure highlighted that there are a number of gaps in the SOCI Act that limit our ability to prepare, prevent and respond to cyber incidents*." [p 33]. It is true that one of these gaps, a focus of the Consultation Paper, is the fact that the SOCI Act applies to critical infrastructure systems and not non-critical infrastructure systems that nonetheless hold other 'business critical data'. There is an opportunity to bring non-critical infrastructure within ambit of the legislation. This will allow the Government an opportunity to close gaps in our current legislative and regulatory framework. Macquarie supports the expansion of the definition of business critical data and does not see significantly expanded regulatory burden by doing so (or, we would argue the regulatory burden, is warranted given the significant risks at play).

32. We have heard some feedback from members of industry that the best place for regulating business critical data is the Privacy Act. We strongly disagree. The Privacy Act does not provide guidance and regulation on how to best store data and respond to breaches. The SOCI regime does. The Government must look beyond an individual rights approach which the Privacy Act provides.

33. Separately, as discussed above regarding IOT devices, we cannot continue to condone holes and exceptions in the cyber security ecosystem especially for large corporate entities such as telecommunications providers. It simply makes no sense. The scenarios given in the Paper on page 41 make this point very clearly. We consider the threshold of systems that hold personal information of at least 20,000 individuals is a reasonable and useful threshold to ensure that regulatory burden is not unnecessarily applied.

34. However, Macquarie submits that while expanding the definition of business critical data we cannot overlook the existing shortcomings of the SOCI Act in this review period. Section 9(2B) of the SOCI Act provides that an asset is not a critical infrastructure asset (and is therefore not a critical data storage or processing asset) if the asset is located outside of Australia.[2] In effect, this provision limits the application of the SOCI Act to critical infrastructure assets located within Australia only. This is a significant risk. the Security of Critical Infrastructure Act 2018 (SOCI) Risk Management Program Rules4 declared that transmission or processing of sensitive operational information outside Australia poses a material risk to Australia's national security.

31. The effect of section 9(2B) therefore provides entities handling critical data (including Government data) with an opportunity to circumnavigate the SOCI Act by storing their data offshore (which would mean that even if the asset otherwise met the definition of a 'critical data storage or processing asset', it would not technically be such an asset that is captured by the SOCI Act by virtue of section 9(2B)). This gap in regulation simply must be resolved given the material risk to Australia's national security. To allow this gap to remain unresolved will create a perverse 'incentive' for Australia's SONS and critical infrastructure entities to proactively shift their data offshore in order to avoid compliance with Australian Law.

[2] s 9(2B) *SOCI Act.*

Measures 6 – 8 Improving our national response to the consequences of significant incidents – Consequence management powers, simplifying how government and industry shares information in crisis situations and Enforcing Obligations

32. In relation to measures 7-8 Macquarie is broadly supportive of what the Paper proposes. But again, we see the ability for a co-regulatory Cyber Alliance Board and its ability to represent industry, be nimble and share with Government as an option which Government should not overlook.

33. The Paper suggests that Government propose to amend SOCI to support a fast and effective approach to the consequences of significant incidents. We submit that the Cyber Alliance board would assist government to help manage the consequences of cyber incidents in a fast and effective manner. Macquarie respectfully submits that consultation on cyber matters to date, has not been fast or efficient.

34. While the Government explores a last resort power that will allow it to direct an entity to take specific actions to manage the consequences of a national significant incident, it cannot overlook the jurisdictional limits of the SOCI Act and section 9(2B) as discussed above at 33.

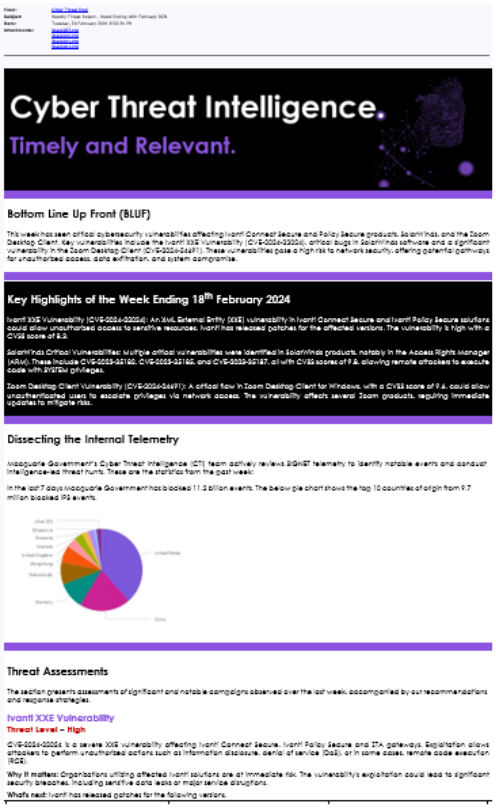
35. In order for the Minister for Cyber Security to be able to effectively manage and review the use of a critical data storage or processing asset in a manner that complies with the SOCI Act and exercise its special powers and the proposed last resort powers under the SOCI Act to protect this critical, sensitive and important information, it should be given powers under the SOCI Act to prevent nationally significant business critical data from being stored offshore. Otherwise we again have a situation where, frankly, there are holes in Australia's cyber security posture. It cannot be the legislative intention that some critical infrastructure providers are beyond the scope of these powers.

Measure 9 - Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act

36. Macquarie again highlights its unique position as a provider of critical infrastructure regulated by SOCI, a owner of SoNs, HCF certified and as a licensed carrier under the *Telecommunications Act 1997* (Cth). We agree that telecommunications assets are an integral and interconnected component of the broader critical infrastructure ecosystem and that legislative harmonisation would address legislative complexities in security and risk mitigation for the sector.

37. Macquarie broadly agrees that there should be consolidation, but does propose that the aim must be harmonisation of the Telecommunications Act and SOCI Act, rather than an expanded list of regulation. We understand from the Department that this is the intent, but again we would be interested in hearing more from the Office of Parliamentary Counsel or Department on any proposed wording.

Appendix A



Cyber Threat Intelligence.

Timely and Relevant.

Bottom Line Up Front (BLUF)

This week has seen critical cybersecurity vulnerabilities affecting Ivanti Connect Secure and Policy Secure products, SolarWinds, and the Zoom Desktop Client. Key vulnerabilities include the Ivanti XXE Vulnerability (CVE-2024-22024), critical bugs in SolarWinds software and a significant vulnerability in the Zoom Desktop Client (CVE-2024-24691). These vulnerabilities pose a high risk to network security, offering potential pathways for unauthorized access, data exfiltration, and system compromise.

Key Highlights of the Week Ending 18th February 2024

Ivanti XXE Vulnerability (CVE-2024-22024): An XML External Entity (XXE) vulnerability in Ivanti Connect Secure and Ivanti Policy Secure solutions could allow unauthorized access to sensitive resources. Ivanti has released patches for the affected versions. The vulnerability is high with a CVSS score of 8.3.

SolarWinds Critical Vulnerabilities: Multiple critical vulnerabilities were identified in SolarWinds products, notably in the Access Rights Manager (ARM). These include CVE-2023-33182, CVE-2023-33182, and CVE-2023-33187, all with CVSS scores of 9.6, allowing remote attackers to execute code with SYSTEM privileges.

Zoom Desktop Client Vulnerability (CVE-2024-24691): A critical flaw in Zoom Desktop Client for Windows, with a CVSS score of 9.6, could allow unauthenticated users to escalate privileges via network access. The vulnerability affects several Zoom products, requiring immediate updates to mitigate risks.

Dissecting the Internal Telemetry

Macquarie Government's Cyber Threat Intelligence (CTI) team actively reviews SIGNET telemetry to identify notable events and conduct intelligence-led threat hunts. These are the statistics from the past week:

In the last 7 days Macquarie Government has blocked 11.3 billion events. The below pie chart shows the top 10 countries of origin from 9.7 million blocked IP2 events.

Threat Assessments

The section presents assessments of significant and notable campaigns observed over the last week, accompanied by our recommendations and response strategies.

Ivanti XXE Vulnerability

Threat Level – High

CVE-2024-22024 is a severe XXE vulnerability affecting Ivanti Connect Secure, Ivanti Policy Secure and ZTA gateways. Exploitation allows attackers to perform unauthorized actions such as information disclosure, denial of service (DoS), or in some cases, remote code execution (RCE).

Why it matters: Organizations utilizing affected Ivanti solutions are at immediate risk. The vulnerability's exploitation could lead to significant security breaches, including sensitive data leaks or major service disruptions.

What's next: Ivanti has released patches for the following versions.

Product	Affected Versions	Fixed Versions
Ivanti Connect Secure	version 9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2, 22.5R1.1, and 22.5R2.2	versions 9.1R14.5, 9.1R17.3, 9.1R18.4, 22.4R2.3, 22.5R1.2, 22.5R2.3 and 22.6R2.3 versions 9.1R12.3, 9.1R16.3, 22.1R6.1, 22.2R6.1, 22.3R1.1 and 22.4R1.1
Ivanti Policy Secure	version 22.5R1.1	versions 9.1R17.2, 9.1R18.4 and 22.5R1.2 versions 9.1R14.3, 22.4R1.1 and 22.4R1.1
ZTA gateway	version 22.5R1.3	versions 22.5R1.4, 22.6R1.2 and 22.6R1.7

Zoom Desktop Client Vulnerability

Threat Level – Critical

The Zoom Desktop Client for Windows, along with the Zoom VDI Client and Zoom Meeting SDK for Windows, are affected by a critical vulnerability identified as CVE-2024-24691. This flaw, due to improper input validation, could allow an unauthenticated attacker to escalate privileges via network access. The vulnerability has been assigned a CVSS score of 9.6, indicating its severe impact potential.

Why it matters: Privilege escalation vulnerabilities are particularly concerning because they can enable attackers to gain elevated access to resources that are normally protected from end users. This could lead to unauthorized actions, such as accessing sensitive information, installing malware, or taking control of affected systems.

What's next: Users and IT administrators are urged to update affected Zoom applications to the latest versions to mitigate this vulnerability. Specifically, updates are available for Zoom Meeting SDK for Windows (version 5.16.2 and later), Zoom Rooms Client for Windows (version 5.17.0 and later), Zoom Desktop Client for Windows (version 5.16.2 and later), and Zoom VDI Client for Windows (version 5.16.10 and later, excluding 5.16.16 and 5.15.12).

Cyber Threat Intelligence Capability Spotlight

Unveiling the unseen, the Macquarie Government's team casts a vigilant eye on global threats affecting Australia's cyber and geopolitical landscapes. Our mission? Safeguarding Australia's digital tomorrow. With access to 42B agency logs, Macquarie Government's Cyber Threat Intelligence (CTI) team gets a unique advantage to assess the threads of internal telemetry into a comprehensive web, exposing hidden threat actors. Our intelligence not only empowers agencies to diminish their risk profile, but also enrich following capabilities:

- **Attack Surface Management** – See your organisations from an attacker's perspective by continuously discovering and assessing vulnerable assets for remediation.
- **Breach Attack Simulation** - Enables organisations to gain a deeper understanding of security posture by safely simulating threat actor tactics, techniques, and procedures to validate security control effectiveness.
- **Cyber Threat Intelligence** – Provides timely and relevant information on threats to agencies assisting agencies in building a Threat-Informed Defence to reduce risk to an agency.
- **SIEM-as-a-Service** - Fully managed, Splunk Enterprise SIEM with automated threat analysis and real-time alerting with meaningful dashboards.
- **SOC-as-a-Service** - 24x7 monitoring and detection by government cleared, Australian based, security engineers.
- **Vulnerability Management-as-a-Service** – Helps organisations adopt highly effective vulnerability management practices to mitigate harmful cyber risks and reduce the impact of security incidents.