NEXTGEN

2023-2030 Australian Cyber Security Strategy Discussion Paper

Submission to the Expert Advisory Board

The NEXTGEN Group (NEXTGEN) is a sovereign Australian company deeply involved in providing a mix of enterprise cyber and data security capabilities in the Asia Pacific. NEXTGEN also supports technological innovation through services specifically designed to help new and emerging IT companies find success.

Summary of recommendations

In this submission to the Expert Advisory Board's (EAB) *2023-2030 Australian Cyber Security Strategy Discussion Paper* (ACSSDP),[1] NEXTGEN offers the following recommendations:

1. **ACSSDP Question 2.b.:**

    a. That the Cyber Security Industry Advisory Committee's (CSIAC) 2022 recommendations to Government about clarifying cyber security responsibilities for business not covered by the *Security of Critical Infrastructure Act 2018* (SOCI 2018), as well as those recommendations regarding the Best Practice Regulations Taskforce, be considered by the EAB for their relevance to the ACSSDP.

    b. That the EAB consider advising Government on how much legislative change is practically useful (and reasonably implementable) for Australia's cyber security?

    c. That data must be included in the definitions of critical infrastructure for Government to achieve its economic and security goals for Australia.

2. **ACSSDP Question 2.c..** That a cyber (and data) security obligation, in the form of efforts to reasonably address security risks and consequences, should be made of company directors (and legal equivalents).

[1] 2023-2030 *Australian Cyber Security Strategy Discussion Paper*, Attachment A.

3. **ACSSDP Question 2.d..** Noting that the Government has multiple, ongoing cyber security related initiatives underway, Government should clearly and compelling state the scope and anticipated value-add of any potential *Cyber Security Act*.

4. **ACSSDP Question 2.e..** That Government should monitor the regulatory burden on business as the result of its interventions in the market. This is best done by an independent, adequately resourced, body or office.

5. **ACSSDP Question 6.:**

   a. That departments and agencies be given reporting obligations that mirror those required of industry under SOCI 2018. Specifically, that departments and agencies attest to Government – formally, publicly, and annually – that they have a cyber security Risk Management Program-like plan that meets the Protective Security Policy Framework, or other benchmark set by Government.
   b. That senior public servants should be held accountable for cyber breaches in their departments or agencies.
   c. That the EAB consider previous recommendations from the Australian National Audit Office (ANAO) and the CSIAC relevant to making Government a cyber security exemplar. This should include the CSIAC's 2022 recommendation that the 'Cyber Hubs' initiative be given "more teeth and … accelerated".[2]

6. **ACSSDP Question 20.:**

   a. That strong, transparent, and independent evaluation and review measures are required for a successful Strategy. However, a robust framework for Australia's cyber security should be broader than the Strategy and have both internal and external evaluation and reporting, including:

      i. The publication of an annual report on the Strategy drawing on CSIAC's 2022 recommendation for a "strong empirically based measurement framework to monitor and gauge the implementation and effectiveness of the initiatives".
      ii. A commitment to a formal review of the Strategy at the midpoint of its proposed life in 2026/2027.
      iii. The continuation of a CSIAC-like body to provide ongoing advice to Government on the Strategy. Membership of this body should broadly reflect the scope of the Strategy, potentially including representation from the public, business, technology, research, and education communities. Additionally, Government should strive for gender and age balance in representation.
      iv. That departments and agencies be given obligations that mirror SOCI 2018's reporting requirements. Specifically, that departments and agencies attest to Government – formally, publicly, and annually – that they have a cyber security Risk Management Program-like plan that meets the *Protective Security Policy Framework*, or other benchmark set

[2] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-IAC-annual-report-2022.pdf, p.7.

by Government. *Note that this recommendation has previously been made under Question 6 (see paragraph 5.a.).*

v. That there should be the continuation, and strengthening, of ANAO cyber security audits of departments and agencies. These audits should include implementation of the Strategy's intent.

vi. That the new Coordinator for Cyber Security be required to annually report on their view of Government's cyber security preparedness, including challenges, appropriate to their role.

This submission does not address Questions: 2.a. and 2.g.; elements of 2.f.; 3.–5.; 7.–14.; and 17.–20.

General

Why listen to NEXTGEN?

NEXTGEN is a sovereign IT, cyber security, and data company which provides a range of services to customers including: cyber and data security and resilience capabilities; cloud services; a cyber lab; and a portfolio of leading enterprise software. NEXTGEN is an expert in, and represents companies who are part of, the IT and data supply chain for Australia's critical infrastructure sectors.

Additionally, NEXTGEN is a growth engine for small to medium IT enterprises, offering support services for emerging IT businesses to help them achieve success through efficient backroom operations, including marketing, sales, billing, and finance.

Finally, NEXTGEN contributes to Australia's IT exports through our presence in New Zealand, Singapore, Indonesia, Malaysia and the Philippines. This presence is part of NEXTGEN's vision to be a significant IT force in the Asia Pacific.

NEXTGEN believes that our submission offers the EAB ground-truthed views on cyber and data security for Australia, as well as on the right balance between growing sovereign cyber security capabilities and the benefits of participation in the global cyber security community.

Question 1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

NEXTGEN believes that the main challenge for the EAB, and subsequently Government, is not so much a challenge of ideas as a challenge of priorities, balance, and implementation, including sufficient resourcing.

NEXTGEN notes that cyber security is dynamic and evolving, and that the threats Australia faces are industrial in scale, global in source, and variable in sophistication. Consequently, the Strategy – particularly given its aspiration to remain relevant until 2030 – has to be open to change. This openness must include to a passion for considering new ideas, the leadership to reprioritise, the flexibility to strike new balances, and a commitment to new resourcing where it is required. Government processes and bureaucracy must be similarly flexible and agile, in practice as well as in policy.

Question 2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

b. Is further reform to the *Security of Critical Infrastructure Act* required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

The CSIAC's *Annual Report 2022*[3] concluded that SOCI 2018 doesn't sufficiently define Australian business' cyber security obligations. Specifically, CSIAC wanted Australian business that isn't covered by SOCI 2018 to have more clarity on their responsibilities. Additionally, CSIAC noted that its recommendations regarding the Best Practice Regulations Taskforce should be considered, and responded to, by Government. NEXTGEN recommends that the EAB examine these CSIAC recommendations to determine their continued relevance to the ACSSDP.

More broadly, Question 2.b. has multiple dependencies, particularly given the EAB's suggestion that Australia might require a *Cyber Security Act*.[4] The question for the EAB to consider as part of the ACSSDP is how much legislative change is practically useful (and reasonably implementable) for Australia's cyber security?

NEXTGEN notes that the SOCI 2018 reforms are fresh and are still being implemented. For example, the Risk Management Program obligations for 13 critical infrastructure asset classes were only triggered on 17 February 2023 and there (reasonably) is an

[3] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-IAC-annual-report-2022.pdf

[4] 2023-2030 *Australian Cyber Security Strategy Discussion Paper*, p. 17 and Attachment A, Question 3.d.

18–month grace period for effective compliance. The challenge Government faces is balancing the uncertainties of how effective its ongoing reforms are, noting also the potential for changes to the *Privacy Act (1998)*, against the need for more legislation.

Regardless, NEXTGEN believes that the Government's economic and security goals for Australia cannot be achieved without the inclusion of 'data' in the definition of critical infrastructure. This position is based on the following:

1. The fact that global data volumes are already massive and are growing massively. It is probable that the importance of data, and threats to it, will also grow.
2. A belief that data is vital to Australia's functioning, and that this importance will only increase with the growth and interconnectivity of IT, Operational Technology, the Internet of Things, and Artificial Intelligence (AI) and Machine Learning (ML). SOCI 2018's inclusion of data processing and storage as a critical infrastructure sector for Australia was prudent. However, this inclusion only really covers the data 'reservoirs' – not the quality and safety of the data that flows to and from them.
3. A belief that data has economic, political, and national security value in, and of, itself. The societal value of individual data is in addition to this.
4. The fact that data provides situational understanding and decision-making advantage, including to groups such as criminals, business and governments. As the Department of Defence stated in the *Defence Data Strategy 2021–2023*, "we have a responsibility to harness the potential of our data and leverage it … to achieve strategic advantage over our competitors".[5] Defence goes on to link data specifically to its decision-making capability.
5. The fact that data is critical for accurate AI and ML training and performance.[6]
6. As indicated by Australian data breaches in the first Quarter of 2023, the fact that breaches of personally identifiable information are individually and politically sensitive.

c. Should the obligations of company directors specifically address cyber security risks and consequences?

NEXTGEN suggests that a cyber security (and data security) obligation, in the form of a requirement to reasonably address security risks and consequences, should be made of company directors (and legal equivalents).

[5] Defence Data Strategy 2021–2023, p. 5.

[6] For example, see Securing the Future of AI and ML at Microsoft - Security documentation | Microsoft Learn

NEXTGEN notes that Government has committed to the goals of making Australia the world's "most cyber secure nation" and a "top 10 digital economy and society" by 2030[7]. It is difficult to see how these goals can be achieved without Government leadership. This leadership presumably includes formal reinforcement that cyber and data security is a cost of doing business in Australia. Otherwise, while economic, reputational, and social responsibility factors should push business towards addressing cyber security and data risk and consequence, the achievement of Government's policy goals may not occur by 2030.

NEXTGEN also notes that SOCI 2018 has created a precedent for cyber security obligations for business, including the obligation for a "board, council or other governing body" to annually report that their Risk Management Program is "approved" and therefore (presumably) funded and fit–for–purpose.[8]

d. Should Australia consider a *Cyber Security Act*, and what should this include?

NEXTGEN believes that the responsibility for answering this question or, at the very least, indicating the left and right of arcs for a potential *Cyber Security Act*, lie with Government.

NEXTGEN notes that there are multiple legislative and policy regimes impacting cyber security already in place, and that these could reasonably be said to lack a desirable degree of consistency. Examples include: the ongoing *Privacy Act 1998* review process;[9] *SOCI 2018* legislation; cyber security guidance of the Therapeutic Goods Administration;[10] and the cyber and data security tender requirements for a government body's cloud migration.[11]

Noting that the Government has multiple, ongoing cyber security related initiatives underway, the scope and anticipated value-add of any potential *Cyber Security Act* should be clearly and compelling stated. Without such intent, this sub-Question asks for thrust without providing vector.

[7] 2023-2030 *Australian Cyber Security Strategy Discussion Paper*, p. 7. and https://www.pmc.gov.au/news/digital-economy-strategy-2022-update-released

[8] SOCI (2018), as amended), Part 2A—Critical infrastructure Risk Management Programs, Section 30AA – Simplified outline of this Part.

[9] Privacy Act Review Report | Attorney-General's Department (ag.gov.au)

[10] https://www.tga.gov.au/how-we-regulate/manufacturing/medical-devices/manufacturer-guidance-specific-types-medical-devices/regulation-software-based-medical-devices/medical-device-cyber-security-guidance-industry

[11] The Australian Maritime Security Agency's REOI-22AMSA097, Invitation for Expressions of Interest – Supply, Design and Implementation of an Integration Capability and Associated Optional Services, dated 19 August 2022.

e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

NEXTGEN believes that a reasonable conclusion from the SOCI 2018 consultations, including submissions to the Parliamentary Joint Committee on Intelligence and Security, is that business is concerned about regulatory burdens. These burdens include the cost of SOCI 2018 compliance as well as the costs of complying with international cyber security, privacy, data and related regulations.

Consequently, NEXTGEN believes it is critical that Government effectively monitors the regulatory burden on business as the result of its interventions in the market. NEXTGEN's position is that this monitoring must be transparent and that this is best done by an independent, adequately resourced, body or office.

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers?

NEXTGEN notes that this sub-question involves complex ethics and legal issues. Beyond this, it is possible that any blanket prohibition on paying ransomware or extortion demands might remove opportunities for the employment of offensive techniques, for example by using negotiation or payment vectors, for law enforcement reasons.[12] While not a recommendation as such, NEXTGEN suggests to the EAB that the judgement of the Australian Federal Police and Australian Signals Directorate should have substantial gravitas in any risk and benefit policy consideration regarding such blanket prohibitions.

[12] While an open source report, the following media coverage of the 2021 Colonial Pipeline ransomware attack implies there are benefits to a flexible approach which enables law enforcement to exploit criminal greed and swim upstream into threat actors: [Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside | OPA | Department of Justice]

Question 6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities? How should we approach future proofing for cyber security technologies out to 2030?

Government as a cyber security exemplar

The SOCI 2018 reform consultations can reasonably be said to have shown concern that the Government is demanding an uplift in industry's cyber security without addressing unresolved cyber security issues in government itself. The reports of the ANAO provide some indication of this,[13] as do reports of cyber breaches involving the Government,[14] and the statement from CSIAC that "the Government has been significantly focussed on what business needs to do to improve its cyber defences. It is also important that government makes progress to harden its own systems and cyber defences".[15]

NEXTGEN supports additional Government initiatives to uplift its own cyber security and better protect Government, Australia's interests, and our citizens. NEXTGEN believes that departments and agencies can better demonstrate and deliver cyber security best practice by:

1. Having obligations that mirror SOCI 2018's reporting obligations on Board-equivalents. That is, that departments and agencies attest to Government – formally, publicly, and annually – that they have a cyber security Risk Management Program–like plan that meets the Protective Security Policy Framework (PSPF), or other benchmark set by Government.
2. Making senior public servants accountable for cyber breaches in their departments and agencies.
3. Having the EAB consider relevant cyber security recommendations from the ANAO and the CSIAC's *Annual Report 2022*, particularly that the 'Cyber Hubs' initiative be given "more teeth and … accelerated".[16]

Future proofing cyber security technologies

NEXTGEN supports any Government intent to future 'proof' cyber security technologies. From our perspective, representing a range of world class cyber security platforms and offerings, we encourage a government culture which is determinedly focused on open engagement with industry, particularly to emerging, innovative, and disruptive

[13] For example, see: https://www.anao.gov.au/work/performance-audit/cyber-security-strategies-non-corporate-commonwealth-entities

[14] For example, see: https://www.abc.net.au/news/2019-02-08/australian-parliament-cyber-security-breach-blame-on-china/10795010

[15] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-IAC-annual-report-2022.pdf, p. 7.

[16] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-IAC-annual-report-2022.pdf, p.7.

technologies. It is through technological and approach innovation (for example, in relation to Zero Trust) that emerging and evolving threats can be better defeated.

Finally, it is our sense that legacy technologies can have a powerful incumbency in government, acknowledging that this can also reflect earned trust and workforce skillsets. Government's risk and opportunity calculus needs to consider how to meaningfully include technological innovation in its processes and acquisitions.

Question 15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

The ACSSDP makes the point that all of society has to be involved for Australia to become the most cyber secure nation in the world by 2030. From NEXTGEN's perspective, measures such as supporting technological research and innovations, as well as compliance regimes are required but insufficient. 'Breaking the food chain' of cybercrime requires a resourced, ongoing, public awareness and education campaign on the importance of cyber security.

The Chief Information Security Officer of the Australian National University has used the term "cyber safety" where it involves students and staff (in preference to 'security'). 'Safety' is believed to resonate more strongly with individuals as being in their interest. Campaigns for wearing seat belts, driving safely, against smoking, and promoting sun safety may be partial examples of what could be done.

Regardless, NEXTGEN sees a need for a clever, evolving, age and situation differentiated campaign – including in schools – to begin shifting Australian attitudes in line with Government's 2030 goal.

Question 16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

As an Australian company, NEXTGEN strongly supports Government's intent to build sovereign cyber security technologies and business. With increasing awareness of the importance of the supply chain as part of a holistic security approach, NEXTGEN suggests that Australia's cyber security ecosystem should be enhanced in its entirety, including research and development; software/hardware creation/production; distribution; systems design and integration; and support. Sovereign technology is not enough.

Noting Government's intent, there is a balance to be struck between building sovereign capabilities and engaging with the knowledge, capabilities, and innovations of the global cyber security community. NEXTGEN notes, for example, the growing calls for the storage and processing of certain data types in Australia. With a rich mixture of sovereign and hyperscale cloud providers offering Australian instances to Government, the Government's decisions on its classified cloud solution will provide a technological and trust lead to others. Such decisions are an example of the current, de facto opportunity for Government to enhance Australia's cyber security technologies ecosystem while also appropriately engaging international providers and partners.

Question 21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

NEXTGEN supports public transparency of, and ongoing input into, the Strategy. Australia's 2016 *Cyber Security Strategy* acknowledged that a static Strategy is analogue thinking for a digital problem: "Recognising that cyberspace is dynamic, the Strategy's initiatives will be reviewed and updated annually and the Strategy reviewed and updated every four years".[17] Unfortunately, there was only a single annual report released.[18]

NEXTGEN believes that strong, transparent, and independent evaluation and review measures are required for the Strategy. The CSIAC's *Annual Report 2022* made a strong statement in support of transparent reporting on the Strategy, stating that evaluation of its impact and value is "crucial" for its success. Following on, CSIAC's recommendation was that any evaluation framework needs to be supported by "a strong empirically based measurement framework to monitor and gauge the implementation and effectiveness of the initiatives under the Strategy, including consideration of an overall maturity index".[19]

NEXTGEN suggests that a robust framework for Australia's cyber security should not just be on the Strategy and should include internal and external evaluation and reporting.

Accepting the economic, social, political and security imperatives for a truly secure cyber future for Australia, NEXTGEN suggests that the following evaluation measures be considered:

1. The publication of an annual report on the Strategy drawing on the CSIAC's recommendation for a "strong empirically based measurement framework to monitor and gauge the implementation and effectiveness of the initiatives".
2. A commitment to a formal review of the Strategy at the midpoint of its proposed life, that is in 2026/2027.

[17] *Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity*, 2016, p.5.
[18] *Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity, First Annual Update 2017*
[19] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-IAC-annual-report-2022.pdf, p. 10.

3. The continuation of a CSIAC-like body to provide ongoing advice to Government on the Strategy. Membership of this body should be broad, for example including representation from the public, business, technology, research, and education communities. Additionally, NEXTGEN would like to see the Government strive for gender and age balance in representation.

4. Require government departments and agencies to attest to Government – formally, publicly, and annually – that they have a SOCI 2018-like cyber security Risk Management Program that meets the *Protective Security Policy Framework* (PSPF), or other benchmark set by Government). *Note that this recommendation has been made already made under a different ACSSDP Question.*

5. The continuation, and strengthening, of ANAO cyber security audits of departments and agencies. These audits should include consideration of the implementation of the Strategy's intent.

6. Requiring the new Coordinator for Cyber Security to annually report on their view of Government's cyber security preparedness, including challenges, facing them in their role.

Outside of formal evaluation and reporting measures, NEXTGEN is involved in, and a strong supporter of, the Trusted Information Sharing Network (TISN). NEXTGEN believes that TISN's subordinate groups, such as the Data Sector Group, are evolving into a valuable resource for sharing industry's experience and perspectives on cyber and data security with government. NEXTGEN appreciates the commitment of the Department of Home Affairs and our industry colleagues to the TISN, and hopes for this to continue.

Conclusion

As a sovereign Australian company, NEXTGEN is grateful for this opportunity to provide input to the ACSSDP. Our best wishes are with the EAB as it considers all submissions and provides advice to Government on how to make Australia the world's most cyber secure nation by 2030.