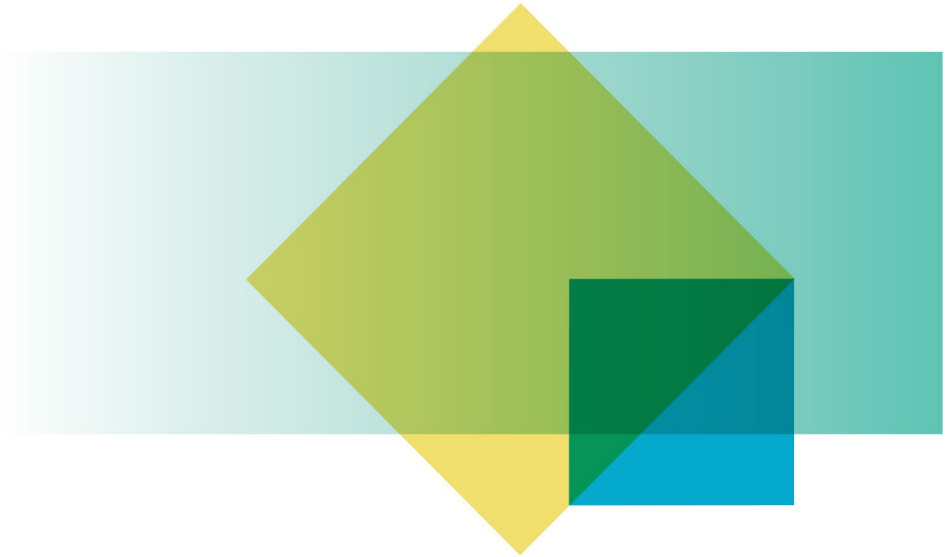
Australian Government

Office of the Australian Information Commissioner

2023–2030 Cyber Security Strategy Discussion Paper

Submission by the Office of the Australian Information Commissioner



Angelene Falk

Australian Information Commissioner and Privacy Commissioner

12 April 2023

OAIC

Introduction

1.1 The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make a submission to the *2023–2030 Australian Cyber Security Strategy Discussion Paper* (Discussion Paper) released by the Department of Home Affairs (Home Affairs) and to contribute to shaping the 2023–2030 Australian Cyber Security Strategy (Strategy).

1.2 The OAIC is Australia's independent Commonwealth privacy regulator.[1] We play a critical role in regulating entities subject to the *Privacy Act 1988* (Privacy Act) to safeguard personal information. The security of personal information is a key regulatory priority for the OAIC.[2]

1.3 Privacy is an essential component in the ring of defence to protect Australia from cyber threats. The Privacy Act includes well-established security requirements, including the obligations under the Australian Privacy Principles (APPs), in particular APP 1 and APP 11, and the Notifiable Data Breaches (NDB) scheme.[3]

1.4 We welcome the Discussion Paper's commitment to considering feedback received on the current review of the Privacy Act by the Attorney-General's Department as part of the development of the Strategy.[4] There is an important opportunity to achieve alignment between the proposals to uplift the established requirements in the *Privacy Act Review: Report 2022* (Privacy Act Review Report) and the new Strategy to ensure a consistent, whole-of-government approach to reducing the risk of cyber harm.[5]

1.5 The development of the Strategy comes at a pivotal time. As the Discussion Paper notes, Australia is still counting the cost of the two most significant data breaches in Australia's history, Optus in September 2022 and Medibank in October 2022.[6] In this context, the OAIC supports additional measures to enhance Australia's cyber security posture. However, as part of this, the OAIC considers it is essential that any cyber security reforms preserve the integrity of the NDB scheme and the OAIC's ability to exercise its powers and functions under the Privacy Act.

1.6 While government plays an important role in providing support, information and resources to assist entities to uplift cyber resilience and security, the primary responsibility for preventing breaches and protecting data in accordance with the Privacy Act rests with the entities themselves.

---

[1] The OAIC is an independent Commonwealth regulator, established to bring together three functions: privacy functions (protecting the privacy of individuals under the *Privacy Act 1988* (Cth), freedom of information (FOI) functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (Cth), and information management functions (as set out in the *Australian Information Commissioner Act 2010* (Cth) (AIC Act).

[2] OAIC, *Priorities for regulatory action 2022–23*, OAIC, accessed 13 March 2023.

[3] See Part IIIC of the Privacy Act.

[4] Home Affairs, *2023–2030 Australian Cyber Security Strategy Discussion Paper*, Home Affairs, Australian Government, 2023, p 14, accessed 22 March 2023.

[5] AGD, *Privacy Act Review: Report 2022*, AGD, Australian Government, 2023, accessed 13 March 2022.

[6] Home Affairs, *2023–2030 Australian Cyber Security Strategy Discussion Paper*, Home Affairs, Australian Government, 2023, p 14, accessed 22 March 2023.

Summary of recommendations

Recommendation 1 – The *2023–2030 Australian Cyber Security Strategy* should consider and align cyber security reforms with proposals in the Privacy Act Review Report to uplift established privacy security obligations and ensure a consistent, whole-of-government approach to reducing the risk of harm. This includes proposals to remove the small business exemption and enhance the NDB scheme's reporting requirements.

Recommendation 2 – Consider the distinct purposes of the various cyber security regulatory frameworks in any reform proposals to ensure that relevant laws continue to work cohesively to address risks of harm without leaving any regulatory gaps.

Recommendation 3 – Collaboration and information sharing mechanisms, supported through legislative amendment where necessary, should be encouraged to reduce the regulatory burden on entities and ensure a consistent, whole-of-government regulatory approach to uplifting Australia's cyber security and resilience.

Recommendation 4 – As a first step to reducing the compliance burdens on industry, consider whether the provision of appropriate guidance could assist entities to navigate their cyber security obligations.

Recommendation 5 – Any proposed amendments to the SOCI Act, specifically in relation to including 'customer data' and 'systems' in the definitions of 'critical assets', should be accompanied by relevant amendments ensuring that protected information can be disclosed to the OAIC so that it can continue to exercise its powers and functions.

Recommendation 6 – Any proposed single reporting portal should be designed in close consultation with affected regulators, to ensure that the timeliness and integrity of the reporting requirements for all the regimes consolidated within the portal, including the NDB scheme, are preserved.

Recommendation 7 – The CSRN and other forums should continue to play a role in post-incident reviews and their work should inform incident response planning policy and practice.

Recommendation 8 – Any proposed obligations of confidentiality should be carefully designed in consultation with regulators, to ensure that agencies such as the OAIC are still able to obtain the information they need from affected entities at the appropriate time, and to exercise their functions and powers in the public interest.

Recommendation 9 – Support government agencies and regulators to engage with international counterparts to influence global dialogues in regulatory areas impacting cyber security, such as privacy, to promote consistently high standards around the world.

Uplifting cyber security through strengthening and streamlining existing frameworks

Strengthening existing frameworks

1.7 Privacy and cyber security are inextricably interwoven. Effective privacy regulation plays an important role in uplifting Australia's cyber security posture, while robust cyber security settings are crucial in protecting Australians' personal information in an increasingly digital environment. In response to Question 1 of the Discussion Paper, we consider that it is important for the Strategy to be built on an understanding of this symbiotic relationship, to succeed in realising the Strategy's goal of making Australia the most cyber secure nation in the world by 2030.[7]

1.8 As recent large-scale data breaches have showed, entities collect and hold an increasingly large quantity of personal and sensitive information about Australians which must be secured effectively. When cyber security settings fail, the risk of harm to individuals whose information is compromised can be devastating.

1.9 The volume and granularity of personal information that is collected by entities, combined with other practices such as tracking, monitoring and profiling, amplifies privacy and security risks. The Privacy Act Review Report considers what changes are needed to Australia's privacy framework to respond to these risks.[8] It includes detailed examination of proposals that would assist in achieving the Discussion Paper's objective of enhancing cyber resilience across the economy.

1.10 Noting the feedback sought in Question 2(a) in relation to the appropriate reform mechanisms to improve mandatory operational cyber security standards across the economy, the OAIC recommends that the new Strategy and any related reforms leverage and build upon the established security requirements in the Privacy Act where appropriate. For example, requirements under APP 1 and APP 11, along with the NDB scheme (explained further below), could be said to provide a 'baseline' level of security protections across the whole economy for personal information.[9]

1.11 Implementation of the reforms proposed in the Privacy Act Review Report also provide an important opportunity to uplift these well-established baseline security obligations.[10] In

---

[7] See Home Affairs, *2023–2030 Australian Cyber Security Strategy Discussion Paper*, Home Affairs, Australian Government, 2023, p 24, 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?'.

[8] See AGD, *Privacy Act Review: Report 2022*, AGD, Australian Government, 2023, Chapter 20, accessed 28 March 2023.

[9] Under APP 1, entities must take reasonable steps beyond technical security measures to protect and ensure the integrity of personal information throughout the information lifecycle, including by implementing strategies in relation to governance, internal practices, processes and systems, and dealing with third party providers. Under APP 11, entities are required to take reasonable steps to protect the personal information they hold from misuse, interference, loss, unauthorised access, modification, or disclosure.

[10] AGD, *Privacy Act Review: Report 2022*, AGD, Australian Government, 2023, accessed 21 March 2023.

particular, the following proposals would aid in achieving the Discussion Paper's objective of enhancing cyber resilience across the economy:

- removing the small business exemption so that small to medium sized enterprises are brought within the Privacy Act's scope, thereby establishing baseline security protections across the entire economy[11]
- strengthening the NDB scheme, including through amendments to the notification requirements and timeframes[12] and an express requirement for entities to take reasonable steps to implement practices, procedures and systems to enable them to respond to data breaches.[13] This will allow the OAIC to take regulatory action quickly to minimise harm to affected individuals and agencies will be able to collaborate more effectively. Affected individuals will also be in a stronger position to mitigate the risk of serious harm arising from the breach. We note that the OAIC has recommended that these proposals could be strengthened through an express obligation on entities to take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach[14]
- including a list of factors in APP 11, which outlines the baseline privacy outcomes APP entities should consider when taking reasonable steps to protect the personal information they hold, setting a bar for entities and encouraging them to conduct continuous analysis of the potential for threats and their severity so that security measures are commensurate to risks[15]
- enhancing the OAIC's Guidelines on APP 11 on the 'reasonable steps' for securing personal information, including cyber-specific elements drawing on technical advice from the Australian Cyber Security Centre (ACSC).[16]

Recommendation 1 – The *2023–2030 Australian Cyber Security Strategy* should consider and align cyber security reforms with proposals in the Privacy Act Review Report to uplift established privacy security obligations and ensure a consistent, whole-of-government approach to reducing the risk of harm. This includes proposals to remove the small business exemption and enhance the NDB scheme's reporting requirements.

[11] See AGD, *Privacy Act Review: Report 2022*, AGD, Australian Government, 2023, Proposal 6.1, accessed 21 March 2023. In response to Question 15(a), which relates government assistance for small business to keep customers' data safe, the OAIC is well placed to support small business to comply with the Privacy Act complementing existing government support.

[12] The proposed amendments would require entities to notify the OAIC and affected individuals within 72 hours of eligible data breaches (rather than the current 30 days) and to set out the steps they have taken or intend to take in response to the breach, including steps to reduce any adverse impacts on the affected individuals.

[13] See AGD, *Privacy Act Review: Report 2022*, AGD, Australian Government, 2023, Proposals 28.2 and 28.3, accessed 21 March 2023.

[14] See Recommendation 106, *Privacy Act Review Discussion Paper: submission by the OAIC*, OAIC, 2021, p 221, accessed 21 March 2023.

[15] See AGD, *Privacy Act Review: Report 2022*, AGD, Australian Government, 2023, Proposal 21.2, accessed 20 March 2023.

[16] See AGD, *Privacy Act Review: Report 2022*, AGD, Australian Government, 2023, Proposal 21.3, accessed 20 March 2023.

Streamlining cyber-security efforts

1.12 The OAIC agrees that if we are to 'lift and sustain cyber resilience and security, it must be an integrated whole-of-nation endeavour'.[17] Having consistent, interoperable and cohesive systems in place is essential to protecting all Australians from cyber threats. Such an approach will promote public trust and confidence in cyber security protections embedded in digital products and services.

1.13 Question 2(d) canvasses whether Australia should consider a Cyber Security Act. The OAIC considers that the concept of a single Act, drawing together cyber-specific legislative obligations and standards across industry and government, offers the potential to simplify regulatory frameworks. We note the Discussion Paper does not provide any further detail and would welcome the opportunity to engage with Home Affairs about the proposed legislation.

1.14 Question 2(e) of the Discussion Paper invites comments on opportunities to streamline existing regulatory frameworks and reduce the burden on industry. The OAIC welcomes certain measures that have already been implemented, such as the establishment of the national Coordinator for Cyber Security and the National Office for Cyber Security.[18] Noting recent experiences with the Medibank and Optus data breaches, we appreciate the need for greater centralisation and coordination of whole-of-government responses to data breaches and cyber incidents.

1.15 The OAIC also supports consideration of streamlining existing frameworks and any duplicative oversight requirements. We acknowledge that entities are currently required to navigate multiple frameworks in relation to cyber security, including the Privacy Act and the *Security of Critical Infrastructure Act 2018* (SOCI Act), as well as frameworks regulated by the Australian Securities and Investment Commission (ASIC),[19] and the Australian Prudential Regulation Authority (APRA).[20]

1.16 While there may be intersections, it is important to acknowledge that these regulatory frameworks address different economic and consumer risks. In this way, the various regimes are essential and complementary components in the ring of defence built to address the risks and harms faced by Australians in the digital age. An enduring and sustainable approach to cyber security must be comprehensive if it is to effectively reduce the harms that can arise from

---

[17] Home Affairs, *2023–2030 Australian Cyber Security Strategy Discussion Paper*, Home Affairs, Australian Government, 2023, p 7, accessed 21 March 2023.

[18] The Hon Clare O'Neil MP, *Prime Minister's Cyber Security Roundtable* [media release], Australian Government, 27 February 2023, accessed 14 March 2023.

[19] *Corporations Act 2001* (Cth), s 912A(1)(h) requires Australian financial services licensees to have adequate risk management systems in place. A failure of the system to manage cybersecurity risks may result in a breach of this obligation: see *ASIC v RI Advice Group Pty Ltd* [2022] FCA 496.

[20] Prudential Standard CPS 234 Information Security requires APRA-regulated entities to take measures to be resilient against information security incidents (including cyber-attacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats. The Standard requires entities to notify APRA of material information security incidents. Prudential Standard CPS 220 Risk Management requires APRA-regulated institutions to have systems for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating material risks that may affect its ability to meet its obligations to depositors and/or policy holders. The Standard requires notification to APRA when an institution becomes aware of a significant breach of, or material deviation from, the risk management framework.

a cyber incident. While we appreciate the need to streamline and centralise frameworks, we would caution that any reforms must ensure that the distinct and important purposes of each regime are considered, to ensure there are no regulatory gaps.

1.17 In addition, the OAIC considers that collaboration and information sharing across government agencies is key to reducing the regulatory burden on entities and ensuring that a consistent, whole-of-government approach is implemented to promote cyber security.[21] A coordinated approach between regulators is central to ensuring that the distinct but complementary cyber regulatory frameworks work cohesively to address risks of harm. The Cyber Security Regulators Network (CSRN), which the OAIC co-chairs with APRA, is an example of a forum that facilitates information sharing between regulators on cyber-related matters, enabling them to reduce duplication in regulatory responses and coordinate messages to regulated entities. Where necessary and appropriate as part of any reform package, greater information sharing and collaboration between regulators should be facilitated by legislative amendment.

1.18 We see the value in regulators working together to avoid unnecessary or inadvertent overlap for industry. At the same time, we do not consider that regulatory overlap is necessarily a negative outcome, particularly where it is well managed. It is more problematic if regulatory gaps expose individuals to harm. In certain circumstances, collaboration between relevant regulators and issuing appropriate guidance to assist entities to understand their regulatory obligations may be more appropriate to address parallel but distinct regulatory concerns, than streamlining frameworks. The new National Office for Cyber Security, announced recently by the Minister for Cyber Security Clare O'Neil MP, is a potential mechanism to centralise and consolidate guidance produced by government agencies and regulators to assist entities.[22]

Recommendation 2 – Consider the distinct purposes of the various cyber security regulatory frameworks in any reform proposals to ensure that relevant laws continue to work cohesively to address risks of harm without leaving any regulatory gaps.

Recommendation 3 – Collaboration and information sharing mechanisms, supported through legislative amendment where necessary, should be encouraged to reduce the regulatory burden on entities and ensure a consistent, whole-of-government regulatory approach to uplifting Australia's cyber security and resilience.

Recommendation 4 – As a first step to reducing the compliance burdens on industry, consider whether the provision of appropriate guidance could assist entities to navigate their cyber security obligations.

[21] The OAIC welcomed the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022*, which came into force on 13 December 2022, that provides greater information sharing powers under the Privacy Act and the AIC Act. These provisions ensure that the OAIC can efficiently and effectively cooperate with other regulators and entities during investigative and regulatory activities. This helps to ensure that duplicative investigation and regulatory responses – both domestically and globally – are avoided and limited resources are directed appropriately.

[22] The Hon Clare O'Neil MP, *Prime Minister's Cyber Security Roundtable* [media release], Australian Government, 27 February 2023, accessed 14 March 2023.

Extending the definition of 'critical assets'

1.19 Question 2(b) of the Discussion Paper invites comments on whether further reform to the SOCI Act is required. In particular, the Discussion Paper seeks feedback on whether existing definitions of 'critical assets' in the Act should be expanded to include 'customer data' and 'systems', the objective being to ensure that the powers under the SOCI Act extend to major data breaches, not just operational disruptions.[23] While we appreciate that this could potentially allow for an uplift of security standards in relation to the handling of personal information, the OAIC is concerned that an unintended consequence of including 'customer data' or 'systems' in the definitions of 'critical assets' would result in a restriction on our ability to exercise our functions and powers in some circumstances, such as in the event of a data breach.

1.20 Although the Discussion Paper does not define 'customer data' or 'systems', it seems likely that it could constitute personal information and/or information about entities' security arrangements and data breaches, and so the potential overlap into areas regulated by the Privacy Act will need to be considered.

1.21 As outlined above, the Privacy Act includes baseline security requirements that play a crucial role in reducing the likelihood of data breaches occurring and in mitigating their impacts on individuals, such as the requirements of APP 1 and APP 11 and the NDB scheme. The Privacy Act applies to regulated entities across the economy, apart from businesses with an annual turnover of $3 million or less (with some exceptions).

1.22 In particular, the NDB scheme requires APP entities to notify the OAIC and affected individuals about data breaches that are likely to result in serious harm to an individual whose personal information is involved. [24] This includes cyber security incidents involving personal information which may also fall within the scope of the SOCI Act.[25] The scheme is designed to enable individuals whose personal information has been compromised in a data breach to take remedial steps to lessen the adverse impacts that might arise from the breach.

1.23 In addition, the Privacy Act includes a complaint mechanism that allows individuals who have been adversely impacted by a data breach to seek redress from the entity that handled their information.[26] This mechanism is crucial as it allows the OAIC to appropriately address the consequences of a data breach for an affected individual. As the trusted national independent privacy regulator, the OAIC plays an important role in providing advice, assurance and, in some cases, a remedy for affected individuals in the event of a breach.

1.24 By contrast, the SOCI Act creates a framework for the regulation of entities in 11 specified 'critical infrastructure' sectors, and imposes mandatory cyber incident reporting to the ACSC to enhance the government's ability to manage national security risks.[27] We note that the SOCI Act

---

[23] See Part 1, Division 1 of the SOCI Act 2018.

[24] See Part IIIC of the Privacy Act, in particular s 26WK in relation to notification obligations to the Information Commissioner and s 26WL in relation to notification obligations to individuals.

[25] See Part 2B of the SOCI Act.

[26] See Part V of the Privacy Act, including s 36.

[27] CISC, *Cyber security incident reporting*, Factsheet, CISC, Home Affairs, Australian Government, 2022, accessed 24 March 2023.

imposes a number of positive security obligations in relation to assets deemed to be 'critical assets', including creating and maintaining a risk management program, and mandatory cyber security incident reporting.[28]

1.25 Importantly, information that is obtained or created in accordance with the SOCI Act is known as 'protected information', and the use and disclosure of this information is limited under the Act. [29] For example, a cyber security incident that is reported under the SOCI Act, is considered 'protected information' under that Act. The SOCI Act prevents the disclosure of protected information unless an exception applies, or the disclosure is otherwise authorised.[30] Currently, there is no exception or authorisation for an entity to disclose protected information to the OAIC in accordance with that entity's statutory obligation to do so.[31]

1.26 The OAIC is therefore concerned that an unintended consequence of an amendment to extend the definition of critical assets would be to restrict entities from sharing certain information with the OAIC, such as information or documents included in risk management programs (outlining security arrangements) and cyber security incident notifications, where that information is protected information under the SOCI Act. This would hamper the OAIC's ability to effectively respond to and investigate data or privacy breaches, unless an exception under Division 3 of the SOCI Act applied.

1.27 This may also impact the ability of the OAIC to effectively investigate and otherwise handle complaints made by individuals in relation to a data breach. [32] A limitation on the OAIC's power to obtain information from entities would significantly impede the OAIC's exercise of its privacy functions and ability to grant remedies to individuals who have suffered harm. For example, if an individual makes a complaint to the OAIC after suffering harm due to a cyber incident or data breach, the proposed amendment to the SOCI Act may prevent the OAIC from collecting the information it needs to assess whether APP 1 and APP 11 have been complied with, if the affected entity claims that the relevant information is protected information.

1.28 The OAIC therefore recommends that any proposed amendments to the SOCI Act and associated reforms carefully consider this possible intersection and include mechanisms to overcome impediments to the OAIC's exercise of its functions and powers. For example, consideration could be given to amending Division 3, Subdivision A of the SOCI Act to include a new provision to provide for the authorised use and disclosure of protected information to the OAIC for the purposes of exercising its regulatory functions and powers under the Privacy Act.[33]

Recommendation 5 – Any proposed amendments to the SOCI Act, specifically in relation to including 'customer data' and 'systems' in the definitions of 'critical assets', should be

[28] See Part 2A and Part 2B of the SOCI Act.

[29] See the definition of protected information in s 5 of the SOCI Act. The 11 critical infrastructure sectors are: Communications, Financial services and markets, Data storage or processing, Defence industry, Higher education and research, Energy, Food and grocery, Health care and medical, Space technology, Transport, Water and sewerage. See *Defining critical infrastructure*, CISC website, 23 February 2023, accessed 29 March 2023.

[30] See SOCI Act, s 45.

[31] See SOCI Act, s 46.

[32] See Part V, Division 1 of the Privacy Act.

[33] This could be modelled on existing s 43AA, or similar.

accompanied by relevant amendments ensuring that protected information can be disclosed to the OAIC so that it can continue to exercise its powers and functions.

Improving government response to major cyber incidents

Single reporting portal

1.29 Question 13(a) proposes a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators. The OAIC is broadly supportive of the concept of a single reporting portal. However, more detail will be needed on how such a portal would function, and in particular on the interplay between the SOCI Act reporting requirements and NDB scheme obligations given the points outlined in the preceding section.

1.30 If adopted, the portal should be designed to ensure the reporting requirements for each regime are incorporated accurately, and the integrity of the NDB reporting scheme is preserved. The portal would also need to enable quick access to reported information by the agencies monitoring compliance with relevant statutes. Potential difficulties would arise if centralised reporting slows or limits the information flows to regulators. This will be crucial to ensuring the OAIC is able to continue to effectively exercise its functions and powers as the trusted national independent privacy regulator, and provide advice, assurance, and, in some cases, a remedy for affected individuals and the public.

1.31 It is also important to note that the NDB scheme is not limited to cyber incidents, and also regulates data breaches that occur across all environments including in physical (not online) environments, for example as a result of human error or system fault.[34] Together with other affected regulators, the OAIC would therefore need to be closely involved in the development of any single portal to ensure that clear messages and processes are developed for regulated entities in relation to how to report different types of incidents.

Recommendation 6 – Any proposed single reporting portal should be designed in close consultation with affected regulators, to ensure that the timeliness and integrity of the reporting requirements for all the regimes consolidated within the portal, including the NDB scheme, are preserved.

Effective post-incident review and consequence management models

1.32 The OAIC is supportive of government efforts to develop an effective post-incident review and consequence management model together with industry as discussed in Question 14. We agree

[34] See *Notifiable Data Breaches Report: January to June 2022*, OAIC website, 10 November 2022, which states that 162 of the 396 data breaches during the reporting period resulted from cyber security incidents (41%).

that sharing 'root cause findings' from investigations of major cyber incidents could be invaluable for shaping regulated entities' incident response policies and plans. In a similar initiative, the OAIC periodically publishes statistical information about notifications received under the NDB scheme to help entities and the public understand privacy risks identified through the scheme, and uses scenario examples based on reported incidents to help guide better practice.[35] We note that this practice is starting to be adopted internationally.[36]

1.33 Related to this question, we note the establishment of the new National Office for Cyber Security.[37] Based on recent experience, the OAIC acknowledges the need for greater centralisation and coordination in responding to major cyber incidents and we are therefore broadly supportive of this mechanism.

1.34 We also note that together with APRA, the OAIC co-chairs the Cyber Security Regulators Network (CSRN), the other members being the Australia Communications and Media Authority (ACMA), the Australian Competition and Consumer Commission (ACCC) and ASIC. The purpose of the CSRN is to enable Australian regulators to work together to understand, respond to and share information about cyber security risks and incidents. The CSRN demonstrates that regulators can work together effectively to address gaps and reduce duplication, and forums such as this should continue to play an important role in cyber post-incident evaluation and analysis as part of any future reforms.

Recommendation 7 – The CSRN and other forums should continue to play a role in post-incident reviews and their work should inform incident response planning policy and practice.

Safe harbour provisions

1.35 Question 8 of the Discussion Paper proposes the introduction of an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) and the ACSC to improve engagement with organisations that experience a cyber incident and allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators.

1.36 While the OAIC appreciates the importance of immediate collaboration and information sharing between affected entities and the ASD/ACSC to facilitate an effective immediate response to cyber incidents, there is a need to balance the facilitation of industry cooperation during an incident with the ability of regulatory agencies to enforce laws and deter non-compliance at an appropriate time. In particular, it is important that any confidentiality obligations do not impede the current reporting obligations under the NDB scheme nor subvert the OAIC's regulatory role. Safe Harbour arrangements could take many forms. The OAIC's view is that any such arrangements need to be developed carefully and subject to clear boundaries so that

[35] OAIC, *Notifiable data breaches publications*, OAIC website, n.d., accessed 28 March 2023.

[36] President Biden's Executive Order 14028 established the Cyber Safety Review Board (CSRB) for the purpose of reviewing major cyber events and making recommendations to drive improvements within the private and public sectors. See *Executive Order on Improving the Nation's Cybersecurity*, EO 14028, The White House, 21 May 2021, accessed 15 March 2023.

[37] The Hon Clare O'Neil MP, *Prime Minister's Cyber Security Roundtable* [media release], Australian Government, 27 February 2023, accessed 14 March 2023.

regulatory activity in the public interest is not impeded. While we appreciate the need to incentivise reporting to the ASD/ACSC and facilitate efforts to contain a breach and minimise the potential harms, entities must comply with their legal obligations under the Privacy Act, including their NDB reporting obligation and the obligation to take reasonable steps to protect their data under APP 11.

Recommendation 8 – Any proposed obligations of confidentiality should be carefully designed in consultation with regulators, to ensure that agencies such as the OAIC are still able to obtain the information they need from affected entities at the appropriate time, and to exercise their functions and powers in the public interest.

International interoperability and enhancing relationships with our neighbours

1.37 Question 3 of the Discussion Paper seeks feedback on how Australia can work with its neighbours to build regional cyber resilience and better respond to cyber incidents. The OAIC considers that information sharing between nations on current cyber security risks, threat actors and best practice has a crucial role to play in achieving these objectives.

1.38 The OAIC's membership of the newly formed Global Privacy Assembly Cybersecurity Sub-Working Group will allow us to leverage offshore technical expertise on cyber security and globally elevate the understanding of best practice strategies.[38] Participation in similar knowledge sharing international cooperation efforts by relevant Australian agencies will leverage international cyber security experience for a domestic context, helping to predict trends in the threat landscape.

1.39 Similarly, Question 5 of the Discussion Paper seeks feedback on how Australia can better contribute to international standards-setting processes in relation to cyber security and shape laws in this area. In our experience, participation and leadership in the global dialogue on privacy and security has allowed the OAIC to shape the international narrative on privacy and security, and to promote globally consistent high standards.

1.40 In addition, implementation of the reforms in the Privacy Act Review will bring Australia more in line with international standards, which will ensure Australia continues to be a major contributor to the global discussion on privacy and security. This will support good cyber security outcomes and provide a foundation for Australia to solidify its role as a global leader on cyber security related matters.

1.41 Having contemporary and fit-for-purpose legislative frameworks will provide Australia with the credibility to influence international standard-setting processes, and shape global understandings on what laws and norms are necessary to uphold responsible state behaviour in relation to cyber security.

[38] Global Privacy Assembly, *Global Privacy Assembly* [website], n.d., accessed 23 March 2023.

Recommendation 9 – Support government agencies and regulators to engage with international counterparts to influence global dialogues in regulatory areas impacting cyber security, such as privacy, to promote consistently high standards around the world.