Australian Government

Office of the Australian Information Commissioner

Consultation on 2023-2030 Australian Cyber Security Strategy: Legislative Reforms

Submission by the Office of the Australian Information Commissioner

Angelene Falk
Australian Information Commissioner

Carly Kind
Australian Privacy Commissioner

8 March 2024

OAIC

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make a submission to the Consultation on proposed new cyber security legislation and on changes to the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act).

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) and other laws[2] to safeguard personal information. This includes the obligation on entities to take reasonable steps to ensure that personal information is appropriately protected from misuse, interference and loss, unauthorised access, modification or disclosure under Australian Privacy Principle (APP 11) and complying with obligations under the Notifiable Data Breach (NDB) scheme.[3] The security of personal information is a key regulatory priority for the OAIC.[4]

3. Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation. The volume and granularity of personal information that is collected by entities, combined with other practices such as profiling, monitoring, tracking, and unnecessary retention of data, amplifies privacy and security risks. Therefore, it is important that Australia can respond to these risks in an appropriate manner.

4. We welcome the Consultation Paper's commitment to coordinating other adjacent programs of work across Government, including the Privacy Act Review. There is an important opportunity to achieve alignment between the proposals in the Government's response to the Privacy Act Review Report[5] to uplift the established requirements in the Privacy Act and the 2023–2030 Australian Cyber Security Strategy (the Strategy) and associated 2023-2030 Australian Cyber Security Action Plan (the Action Plan) to ensure a consistent, whole-of-government approach to reducing the risk of cyber harm.

5. Our principal concern is ensuring that the OAIC's regulatory remit is preserved, particularly in relation to the NDB scheme, and more broadly that privacy matters have been given appropriate consideration to ensure the cohesion of the reforms and to provide a consistent framework of obligations and expectations for regulated entities. The OAIC has an important role to ensure that appropriate steps are taken to mitigate harms to individuals arising from cyber security incidents.

6. Effective cyber security practices require entities to adhere to privacy-by-design across the information lifecycle, as entities collect, hold, use, disclose and destroy or de-identify personal information. Entities can help mitigate security risks and harm to individuals that can result from cyber security incidents by minimising the amount of personal information they collect and

---

[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] We note that a number of other Australian laws other than the Privacy Act 1988 also relate to privacy see: www.oaic.gov.au/privacy/privacy-legislation/related-legislation.

[3] See *Privacy Act 1988* (Cth) sch 1 and Part IIIC.

[4] OAIC, *Priorities for regulatory action 2022–23*, OAIC, accessed 25 January 2024.

[5] AGD, *Government Response to Privacy Act Review: Report*, AGD, Australian Government, 2023, accessed 25 January 2024

destroying personal information when it is no longer needed. Minimising collection of data to only the amount necessary to achieve a specific purpose should be part of entities' cyber security strategies. In addition, the OAIC supports the proposed uplift in the Privacy Act Review through a new requirement that collections, uses and disclosures of personal information are fair and reasonable, providing a greater obligation on entities to ensure good privacy practices.

7. An entity can further reduce the risk of harms to individuals and the impact of a data breach by ensuring that they are transparent when a data breach occurs. The primary purpose of the NDB scheme is to ensure individuals are notified if their personal information is involved in a data breach that is likely to result in serious harm. This has a practical function to enable individuals, once notified about a data breach, to take steps to reduce their risk of harm.

8. As an independent statutory office, the OAIC is well-placed to provide its regulatory expertise and highlight the potential impact of these proposals and support Australian government agencies to achieve policy outcomes in the public interest. While the OAIC and government play an important role in providing support, information and resources to assist entities to uplift cyber resilience and security practices, the primary responsibility for preventing breaches and protecting personal information in accordance with the Privacy Act rests with the entities themselves.

9. In this submission, the OAIC outlines it support for addressing gaps in existing regulatory frameworks and amendments to the SOCI Act. We make six recommendations to assist the Department of Home Affairs in ensuring the interoperability of these frameworks with the Privacy Act.

Part 1: New cyber security legislation

10. The OAIC is broadly supportive of the proposed new initiatives intended to achieve improved security outcomes and mitigate harms in Australia's existing legislative and regulatory framework for cyber security. At the same time, it is essential that the complementary reforms proposed under the Privacy Act Review, including in particular recommendations in relation to the security, destruction and retention of personal information, are progressed as a priority in order to uplift cyber security practices.

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

11. Internet of Things (IoT) devices offer important benefits and opportunities to the Australian economy, but they can also carry significant security and privacy risks. As IoT becomes more widespread and integrated into our daily lives, it is imperative that these devices are designed with strong security and privacy features to protect against threats, which may put individual's personal information at risk.

12. The OAIC welcomes the Government's initiative to adopt international standards for consumer-grade IoT devices by working with industry to co-design a mandatory cyber security standard, ensuring that entities and individuals can trust that digital products and services they rely on are secure. It is essential that responsibility for cyber security is appropriately aligned within our digital ecosystem with those that are best placed to reduce risks. Many entities and individuals do not have the capability or expertise to assess the security standard of products and services. Entities and individuals rely on products and services which may have inherent vulnerabilities in their

design that can be exploited, and it is no longer sustainable to expect them to be on constant guard to protect their security.

13. The OAIC acknowledges that, having regard to a security by design approach, the first three principles of the ETSI EN 303 645 standard may be an appropriate minimum standard to mandate for consumer-grade IoT devices sold in Australia. The principles are:

    - ensure that smart devices do not have universal default passwords;
    - implement a means to receive reports of cyber vulnerabilities in smart devices; and
    - provide information on minimum security update periods for software in smart devices.

14. That being said, it is important that privacy by design is factored into the design of consumer-grade IoT devices. Adopting a privacy by design approach, in addition to a security by design approach, embeds good privacy practices into the design specification and architecture of IoT devices to ensure that privacy is also considered at the start of the lifecycle of IoT devices. This will allow individuals to engage with products and services with confidence that – like a safety standard – privacy protection is given.

15. Embedding privacy into the design of IoT devices from the start is fundamental to enabling individuals to self-manage their privacy and making entities more accountable for their use of personal information. This goes beyond security of personal information, to cover the handling of personal information throughout its lifecycle, including minimising the collection of personal information and ensuring it is destroyed when no longer needed. To effectively protect personal information throughout its lifecycle, the design process should consider when and how personal information is being collected and stored. This includes considering whether it is actually necessary to collect and hold personal information, strategies to protect personal information and destruction or de-identification of personal information when it is no longer needed.

16. The OAIC considers that it is better to manage privacy risks proactively by embedding good privacy and security practices into design specification and architecture of IoT devices, rather than to retrospectively alter them to address privacy and security risks that come to light.

17. Any guidance or product standards developed under this initiative would need to be carefully designed so as to ensure interoperability with existing privacy obligations or any requirements that are being considered under the Privacy Act Review.

18. Current mandatory requirements for regulated entities include taking reasonable steps to ensure that personal information is appropriately protected from misuse, interference and loss, unauthorised access, modification or disclosure under APP11 and the obligation to take a 'privacy by design' approach by taking reasonable steps to implement practices, procedures and systems to ensure that regulated entities manage personal information in an open and transparent way under APP 1.

19. Relevantly, in relation to the security and retention of data, the Government has agreed in principle in its response to the Privacy Act Review:

    - that APP 11 should be amended to include a list which outlines the baseline privacy outcomes APP entities should consider when taking reasonable steps to protect the personal information they hold (proposal 21.2).

- that organisations should be required to establish maximum and minimum retention periods for personal information, and specify these in their privacy policies (proposals 21.7 and 21.8).
- to review all legal provisions requiring retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information (proposal 21.6).
- that the small business exemption under the Privacy Act should be removed in light of the privacy risks applicable in the digital environment (proposal 6.1).
- that an entity should be required to notify the Information Commissioner not later than 72 hours after becoming aware that there are reasonable grounds to believe there has been an eligible data breach, notify individuals as soon as practicable, including providing information to individuals in phases if it is not practicable to provide the information at the same time, and take reasonable steps to implement practices, procedures and systems to respond to a data breach (proposal 28.2).
- that an entity should be required to set out the steps taken or to be taken in response to a data breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates (proposal 28.3).
- to enhance privacy protections to private sector employees, including by notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm (proposal 7.1).

20. The OAIC supports these proposals as important measures, which would uplift the security practices of regulated entities. In particular, the OAIC supports the removal of the small business exemption, noting that a significant proportion of businesses in Australia are not subject to the Privacy Act.[6]

21. Any guidance or product standards under the initiative to adopt international standards for consumer-grade IoT devices should be developed having regard these proposals.

Recommendation 1 –Progress reforms which have been agreed and agreed in principle in the Privacy Act Review Report as a matter of priority to uplift established privacy security obligations and ensure a consistent, whole-of-government approach to reducing the risk of harm. This includes removing the small business exemption and enhancing the NDB scheme's reporting requirements.

Recommendation 2 – That any minimum standard to mandate for consumer-grade IoT devices sold in Australia is carefully designed so that it is interoperable with existing obligations under the Privacy Act and has regard to the reforms in this area.

[6] As at June 2021, it was estimated that less than 5 per cent of businesses actively trading in the Australian economy had an annual turnover of more than $3 million and consequently obligations under the Privacy Act. This estimate was prepared for the OAIC using ABS counts of Australian Businesses, including entries and exits. Note this estimate does not include exceptions to the small business exemption.

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

22. As part of a range of measures in the Australian Cyber Security Strategy 2023-2030, the Australian Government supports the development of a 'limited use' obligation.[7] The OAIC welcomes the Australian Government's decision to pursue a 'limited use' obligation rather than a 'safe harbour' as this aligns with the Australian community's expectation that entities comply with their legal obligations and are subject to appropriate regulatory oversight.

23. A 'limited use' obligation seeks to encourage industry to share information with the Australian Signals Directorate (ASD) or the National Cyber Security Coordinator (NCSC) following a cyber incident, by providing comfort to industry that the information will not be used for compliance or punitive purposes.

24. The OAIC's view is that any 'limited use' obligation needs to be developed carefully and subject to clear boundaries to ensure that regulatory activity post-containment of the cyber incident in the public interest is not impeded. In particular, it is important that any confidentiality obligations are interoperable with the current reporting obligations under the OAIC's NDB scheme and do not subvert the OAIC's regulatory role, and to ensure that regulators have broader intelligence around the current cyber security threat landscape.

25. It is essential that there is a distinction between information provided by an entity to the ASD, and any information generated by the ASD which should be more broadly accessible to regulators in order for regulators to execute their role effectively. For example, the OAIC would benefit from routinely receiving intelligence reports for a number of reasons within its regulatory remit, including encouraging an entity's compliance with the NDB scheme, deterring non-compliance and accordingly prevent harms from occurring in the first place, identifying emerging issues, and gaining a broader understanding of the threat landscape to enhance our strategic capability.

26. Ultimately, entities must comply with their legal obligations under the Privacy Act, including their reporting requirements and obligation to take reasonable steps to protect their personal information under APP 11. This is to ensure that the harms and privacy impacts on individuals whose information has been compromised due to a cyber incident are minimised. The OAIC will prioritise regulatory action where there may be serious failures to take reasonable steps to protect personal information, the use of inappropriate data retention practices or failures to comply with reporting requirements of the NDB scheme, particularly where risks and mitigations have previously been publicised by the OAIC. Reasonable steps to protect personal information under APP 11 may, depending on the circumstances, require entities to engage and cooperate with the ASD or the NCSC. Accordingly, given the Australian community often seek information from the OAIC following a data breach, it is appropriate for the OAIC to obtain information and assurances that where there is a cyber security incident, the entity involved is cooperating with the ASD and/or the NCSC.

[7] Department of Home Affairs, *2023-2030 Australian Cyber Security Strategy Action Plan*, p 9; Department of Home Affairs, *2023-2030 Australian Cyber Security Strategy Action Plan*, p 26.

27. The OAIC appreciates that industry may be reluctant to share detailed incident information, and that this can reduce the Government's visibility of cyber threats and ability to offer support to entities and individuals during an incident. While a limited use obligation may encourage this industry engagement the ASD and the NCSC, there is a need to take a proportionate response in ensuring industry engagement following an incident with the ability of regulators to take enforcement steps at an appropriate time. The general educational and deterrent value of regulators taking strategic action and the uplift in practice it can bring across the regulated community should also be acknowledged.

28. The OAIC's understanding is that the proposed limited use obligation is not intended to impact regulatory or law enforcement actions or provide immunity from legal liability. A mechanism of this kind will need to be carefully designed in consultation with regulators to ensure that it achieves this objective of balancing effective regulation with access to trusted support.

Recommendation 3 – That the limited use mechanism is carefully designed in consultation with regulators so that it does not preclude regulatory action in the public interest or impact any legislative reporting requirements, including for the OAIC.

Part 2: Amendments to the Security of Critical Infrastructure Act 2018

29. The OAIC is broadly supportive of the proposed amendments to the SOCI Act and the additional references to more fully acknowledge the intersection of the proposed amendments with the operation of the Privacy Act and ongoing Privacy Act Review.

Measure 5: Protecting critical infrastructure – Data storage systems and business critical data

30. The OAIC broadly supports the proposal to strengthen obligations on critical infrastructure entities to protect their data storage systems where security vulnerabilities can have an impact on critical infrastructure.

31. The OAIC supports the statement in the Consultation Paper acknowledging the role of the Privacy Act as the primary legislative framework regulating personal information, as it applies to both critical infrastructure entities regulated by the SOCI Act and non-critical infrastructure entities.[8] It is the OAIC's understanding that the amendment would be interoperable with existing and proposed obligations under APP 11 of the Privacy Act, by imposing additional risk-based requirements on critical infrastructure entities which are also holding large data sets of personal information.

32. The OAIC welcomes the Department of Home Affairs commitment to working closely with the Attorney-General's Department to ensure amendments are complementary to and interoperable with existing and proposed obligations under the Privacy Act.

33. The OAIC supports the proposal that appropriate guidance material is developed to support regulated entities in complying with obligations under the SOCI Act and the Privacy Act. We note that this would be complementary to Privacy Act Review proposal 21.3, which proposes to enhance the OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information.[9] To minimise the impact of regulatory burden, entities will require clear risk-based guidance as to how they can meet their obligations under the SOCI Act and the Privacy Act.

Recommendation 4 – That the OAIC is consulted on the development of guidance material on the relationship between the SOCI Act and Privacy Act.

Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers

34. The OAIC is broadly supportive of measures which support post-incident consequence management. The OAIC is supportive of a directions power of last resort, which may only be

[8] Department of Home Affairs, *2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper*, p 36.

[9] AGD, Privacy Act Review Report, p 22.

authorised by the Minister for Home Affairs (the Minister) if there is no existing power available to support a fast and effective response.

35. The OAIC welcomes that the use of the directions power will not interfere with or impede regulatory action by the OAIC, and a direction should not duplicate or be inconsistent with obligations under the NDB scheme.

36. The Consultation Paper notes that, pursuant to proposal 28.4 in the Privacy Act Review Report, the Government has agreed to introduce a provision to enable the Attorney-General to authorise the sharing of personal information with appropriate entities to reduce the risk of harm in the event of an eligible data breach for specified purposes and for a limited duration.[10] A declaration made by the Attorney-General under the proposed provision in the Privacy Act would take precedence over the SOCI Act directions power in relation to sharing personal information.

37. It should be noted that under the Privacy Act, the Australian Information Commissioner can currently make declarations requiring a respondent to redress loss or damage suffered by a complainant. Additionally, proposed changes under proposal 25.5 in the Privacy Act Review Report, recommend the inclusion of an express provision in the Privacy Act to allow the Australian Information Commissioner to require a respondent to take reasonable steps to mitigate future loss.[11] That said, the existing declarations power (and the Privacy Act Review proposal) are only available in the context of a privacy determination by the Commissioner under s 52 of the Privacy Act as resolution to a privacy complaint or commissioner initiated investigation.

38. As noted in recommendation 1 above, the OAIC recommends that the government progress reforms to the Privacy Act as a matter of priority to support initiatives aimed at uplifting the cyber security posture of Australian entities. The OAIC also recommends giving consideration to other measures to ensure the consequences and harms resulting from the loss of individual's personal information are minimised, and individuals can take action quickly (such as obtaining new credentials) to mitigate any further risks without the need for a privacy determination. Accordingly, the OAIC recommends additional consequent management measures, such as entities being required to take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach. The OAIC welcomes the Government's acknowledgment in the Privacy Act Review Report that further consultation should be undertaken on whether entities should be required to take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.[12]

39. The proposed directions power in the SOCI Act might be used as a 'last resort' to direct an entity to share personal information (for example, where the Minister for Home Affairs is satisfied that the responsible entity is unwilling or unable to address the consequences that prejudice the socioeconomic stability, national security or defence of Australia) and the Attorney-General has authorised this under the Privacy Act. As such, the proposed consequence management power in the SOCI Act will complement the Information Commissioner's existing powers, supporting a more immediate response to a cyber incident.

[10] AGD, Privacy Act Review Report, p 37.

[11] AGD, Privacy Act Review Report, p 36.

[12] AGD, Privacy Act Review Report, p. 9.

40. The paper notes that, if the Government considers using this power, whole-of-Australian-government coordination mechanisms would be convened, including consultation with other government agencies, regulators and law enforcement bodies.

41. If the use of the power is in relation to the collection, use and disclosure of personal information, the OAIC's view is that an appropriate safeguard should include mandatory consultation with the Australian Information Commissioner. There is precedent for such consultation requirements in other legislation for example, s 53 of the *Office of the National Intelligence Act 2018* (Cth), s 355-72 of the *Taxation Administration Act 1953* (Cth) and s 56AD of the *Competition and Consumer Act 2010* (Cth). This consultation will help ensure strong privacy and security safeguards are included in any direction given by the Minister for Home Affairs, including for example, that only the minimum amount of personal information necessary to achieve the purpose is shared.

Recommendation 5 – That a directions power under the SOCI Act includes explicit, mandatory consultation with the Australian Information Commissioner, as the regulator with primary responsibility for privacy functions conferred by the Privacy Act, in relation to any privacy impacts of a proposed exercise of the directions power.

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions

42. The OAIC considers that the SOCI Act reform presents an opportunity to facilitate information sharing to promote regulatory efficiency and co-operation, and clarifying that entities should take a harms-based approach to decision-making when disclosing information. This is particularly relevant where reporting obligations are enlivened under both the Privacy Act's NDB scheme and the SOCI Act. Where this occurs, there may be benefits in sharing information with other regulatory agencies to ensure the OAIC and other regulators have access to information relevant to decision making and reducing the harms to the Australian public.

43. The OAIC welcomes amendments that would authorise the use and disclosure of protected information to the OAIC for a cyber incident that is also a notifiable data breach. The identification of data breaches is imperative to ensuring that any impact on individuals' privacy can be mitigated as quickly as possible.

44. Disclosure of protected information within government may facilitate effective multi-agency responses to significant incidents including major cyber-attacks and natural disasters.

45. Where a government entity proposes to disclose protected information which includes personal information, additional protections are required to reduce the risks of further harms to individuals. When sharing protected information includes personal information, only the minimum amount of personal information necessary to achieve the specific purpose should be shared.

46. The taking of a harms focused and outcomes-based approach to deciding whether information should be shared, and what types of information should be shared and for what purpose, will help ensure that any further potential harms on individuals are minimised.

Recommendation 6 – The OAIC welcomes the taking of a harms focused and outcomes-based approach to sharing protected information under the SOCI Act. Where protected information includes personal information, data minimisation principles which limit the data to what is reasonably needed, for a specific purpose and for a specified period of time, should be applied.