Law Council
OF AUSTRALIA

2023-2030 Australian Cyber Security Strategy

Department of Home Affairs

5 May 2023

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia represents the legal profession at the national level, speaks on behalf of its Constituent Bodies on federal, national and international issues, and promotes the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world. The Law Council was established in 1933, and represents its Constituent Bodies: 16 Australian State and Territory law societies and bar associations, and Law Firms Australia. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Law Society of the Australian Capital Territory
- New South Wales Bar Association
- Law Society of New South Wales
- Northern Territory Bar Association
- Law Society Northern Territory
- Bar Association of Queensland
- Queensland Law Society
- South Australian Bar Association
- Law Society of South Australia
- Tasmanian Bar
- Law Society of Tasmania
- The Victorian Bar Incorporated
- Law Institute of Victoria
- Western Australian Bar Association
- Law Society of Western Australia
- Law Firms Australia

Through this representation, the Law Council acts on behalf of more than 90,000 Australian lawyers.

The Law Council is governed by a Board of 23 Directors: one from each of the Constituent Bodies, and six elected Executive members. The Directors meet quarterly to set objectives, policy, and priorities for the Law Council. Between Directors' meetings, responsibility for the policies and governance of the Law Council is exercised by the Executive members, led by the President who normally serves a one-year term. The Board of Directors elects the Executive members.

The members of the Law Council Executive for 2023 are:

- Mr Luke Murphy, President
- Mr Greg McIntyre SC, President-elect
- Ms Juliana Warner, Treasurer
- Ms Elizabeth Carroll, Executive Member
- Ms Elizabeth Shearer, Executive Member
- Ms Tania Wolff, Executive Member

The Chief Executive Officer of the Law Council is Dr James Popple. The Secretariat serves the Law Council nationally and is based in Canberra.

The Law Council's website is www.lawcouncil.asn.au.

Acknowledgement

The Law Council is appreciative of the contributions of the following bodies to this submission:

- Law Institute of Victoria;
- Queensland Law Society;
- Law Society of New South Wales; and
- The Business Law Section's Corporations and Digital Commerce Committee.

Executive Summary

1. The Law Council welcomes the opportunity to respond to the Department of Home Affairs' Discussion Paper titled *2023-2030 Australian Cyber Security Strategy* (**Discussion Paper**).

2. The Law Council supports detailed consideration of initiatives that can drive behavioural and cultural change through the appropriate balance of regulatory intervention and industry-led best practice. Noting that many of the specific initiatives canvassed in the Discussion Paper are proposed at a high level, there will be an ongoing need to consider specific recommendations for reform through future consultation with stakeholders. The Law Council considers that this Discussion Paper should serve as a precursor to subsequent detailed consultations.

3. The Cyber Security Strategy should play a helpful role in identifying the key principles and challenges emerging from the parallel proposals, reforms and review processes taking place in relation to privacy, data protection and cyber security regulation across the economy.

4. The Law Council emphasises the need to ensure proportionality, consistency, and certainty within the regulatory landscape. Disjointed and siloed reforms in response to cyber threats will not achieve this goal. Regulatory and procedural certainty is critical in the aftermath of a cyberattack where the timeframe to make decisions and to respond appropriately is significantly constrained.

5. Whilst the Law Council recognises the need for an overarching framework for cyber security regulation, it submits that any such regulatory framework must be appropriately balanced so as not to unduly discourage innovation, and investment in innovation, in Australia.

6. It is vital to the strength of Australia's cyber security that education is encouraged at all levels of the market, from consumers to company directors (in particular small and medium enterprise), to reduce the siloed nature of cyber security expertise and encourage a level of responsibility and accountability for threats.

7. In the limited time available for consultation, the Law Council has selectively responded to some of the questions set out in the Discussion Paper based on the interest and expertise of its Constituent Bodies and expert advisory committees.

8. In outline, the Law Council's submission addresses the following key matters:

    - there is a need for the Cyber Security Strategy to address more fully the following areas:
        - general principles of regulatory best practice to guide reform; and
        - less invasive alternatives to verify identity and minimise personal information held by private businesses;
    - consideration is needed in relation to further legislative and non-legislative measures to address electronic funds transfer payment fraud;
    - in assessing appropriate mechanism for reforms to improve mandatory operational cyber security standards, the following two considerations should be addressed:
        - the need for cyber security agility; and

- the need to appropriately define the different roles of actors when managing cyber security risks across the supply chain;

- expanding the definition of critical assets under the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**) to include customer data has in-principle support, and should be further considered. However, any changes should be preceded by a holistic assessment of the regulatory burden and certainty of the SOCI regime;
- the Law Council has generally favoured voluntary principles-based governance standards relating to cyber security over new legislated obligations on company directors as it represents an agile and responsive approach to managing cyber security risk through corporate governance;
- the Law Council reserves its position on the desirability of a Cyber Security Act, noting the limited context provided in the Discussion Paper. However, the Law Council supports further consultation on this issue, and makes some suggestions for the potential scope of a Cyber Security Act;
- the Law Council reserves its position in relation to a prohibition on the payment of ransoms and extortion demands by victims of cyberattacks or insurers, noting that any prohibition would be a world-first and requires detailed consideration. To promote further iterative consultation, the Law Council suggests any proposal to introduce a prohibition must clearly establish an evidence base on the necessity of a prohibition, be accompanied by detailed impact analysis, consider appropriate exceptions, and should occur in a phased manner in consultation with all stakeholders;
- there is general support for amending the Notifiable Data Breach scheme to establish a voluntary or preliminary notification scheme whereby an APP entity may notify the Office of the Australian Information Commissioner (**OAIC**) on a voluntary or preliminary basis, and then within an appropriate time period (reflective of how most matters require a sense of urgency and promptness), communicating with the OAIC whether the APP entity considers that data breach to be one that is 'likely to result in serious harm';
- a single reporting portal for all cyber incidents is desirable, and would assist in harmonising existing requirements to report separately to multiple regulators; and
- transparency and robust evaluation measures within the Cyber Security Strategy are critical. Robust parameters are required, including independent oversight of government agencies in relation to progress against data security standards including the Protective Security Police Framework (**PSPF**).

Introduction

9. The Law Council's submission is informed by the following key cyber security trends identified by the Australian Cyber Security Centre (**ACSC**) Annual Cyber Threat Report:[1]

    - **increasing number and sophistication of cyber threats** – the ACSC received over 76,000 cybercrime reports, an increase of nearly 13 per cent from the previous financial year;
    - **cyberspace has become a battle ground** – there is increasing risk that regional dynamics in the Indo-Pacific will lead to greater use of cyber operations by states to challenge the sovereignty of others;
    - **Australia's prosperity is attractive to cyber criminals** – Australia is a relatively wealthy country. In 2021–22, cybercrimes directed at individuals, such as online banking and shopping compromise, remained among the most common, while Business Email Compromise trended towards targeting high value transactions like property settlements;
    - **ransomware remains the most destructive cybercrime** – the business model of ransomware groups continues to evolve with significant changes in tactics (e.g., the emergence of combining data encryption and threats to publicly release sensitive information as a method of pressuring ransomware victims into paying, a process which is known as 'double extortion') and the increasing prominence of ransomware-as-a-Service (which is a business model between ransomware operators and affiliates in which affiliates pay to launch ransomware attacks developed by operators).
    - **worldwide, critical infrastructure networks are increasingly targeted** – both state actors and cybercriminals view critical infrastructure as an attractive target; and
    - **the rapid exploitation of critical public vulnerabilities became the norm** – in the past year, Australian organisations and individuals, were indiscriminately targeted by malicious cyber actors who scanned for any network with unpatched systems, sometimes seeking to use these as entry points for higher value targets.

10. The Law Council agrees that lifting and sustaining cyber resilience and security must be an 'integrated whole-of-nation endeavour.'[2] To that end, the Law Council commends the approach taken in the Discussion Paper in laying the groundwork to holistically address a broad range of cyber security issues, from harmonising regulatory frameworks, strengthening Australia's international strategy on cyber security, securing government systems and increasing community awareness of support for victims.

11. Unfortunately, due in part to a piecemeal approach to reform over successive years, Australia's current regulatory framework for privacy and cyber security is fragmented across different sectors of the economy and, for this reason, can at times be difficult to comprehend and apply. Some of the key areas of evolution in the privacy and cyber security landscape include:

    - **ongoing consideration of the adequacy of the Privacy Act 1988 (Cth) (Privacy Act)**: historically, there has been a fragmented approach to reforms

[1] Commonwealth of Australia, Australian Cyber Security Centre, July 2021-June 2022 Annual Cyber Threat Report (March 2023) 11.
[2] Discussion Paper, 7.

to privacy laws, both in terms of the collection and control of personal information, and enforcement options for serious breaches. On 16 February 2023, the Attorney-General publicly released the Privacy Act Review Report[3] for consultation. The Law Council has provided the Attorney-General's Department a detailed response to this review;[4]

- **reforms to Australian Prudential Regulation Authority (APRA) and Australian Competition and Consumer Commission (ACCC) regulated entities relating to cybersecurity**: currently there is a network of overlapping governance requirements for managing cyber security risks, including through the Privacy Act, director's duties, APRA prudential standards. By way of illustration, APRA has its own set of Prudential Standards for the governance and management of cyber security risk (e.g., CPS 234: this standard requires entities to maintain a secure information security capability commensurate with anticipated information security vulnerabilities and threats);[5]
- **specific sectoral obligations including reforms to telecommunications sector security**: and sector specific obligations such as those imposed on telecommunications providers;[6]
- **ongoing consideration of legislative responses to ransomware**: noting proposals in the previous parliament in relation to new and aggravated offences relating to ransomware;[7]
- **inconsistent reporting obligations**: inconsistencies in how entities are required to report on cyber incidents, including in terms of time frames, materiality thresholds and types of agencies and regulators to be notified - especially in industries that are already heavily regulated; and
- **the expanding ambit of the security of critical infrastructure regime**: an expanding list of organisations being brought into the Security of Critical Infrastructure framework, either directly or as part of a supply chain for infrastructure assets with national significance.

12. Historically, it has been said that there is 'no privacy without security', however, because of the proliferating risk of cyberattacks, there is an increasing shift towards a view that there is 'no security without privacy.' This paradigm shift recognises that responding prudently to this exponential increase in risk means ensuring that systems are designed to mitigate the adverse privacy impacts of cyberattacks. Practices such as data minimisation, secure deletion, de-identification and centralised verification are all relevant to achieving this objective.

13. It is important to note that these areas of evolving regulation have created duplicative obligations, where in some cases, two regulatory regimes require the same or similar actions to be taken. By way of illustration, the Telecommunications

[3] Commonwealth of Australia, Attorney-General's Department, Privacy Act Review Report (16 February 2023). ('Law Council Privacy Submission')
[4] Law Council of Australia, Submission to the Attorney-General's Department, Government response to the Privacy Act Review Report (13 April 2023).
[5] Australian Prudential Regulation Authority, Prudential Standard CPS 234 – Information Security (July 2019).
[6] For example, Section 313 of the *Telecommunications Act 1997* (Cth) places an obligation on Carriers and Carrier Service Providers to 'do their best' to: prevent telecommunications networks and facilities from being used to commit offences under laws of the Commonwealth or the States and Territories and protect telecommunications networks and facilities from unauthorised interference and access for the purposes of security. More generally, Part 14 of the *Telecommunications Act 1997* is a regulatory framework which manages the national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities. It is also known as the Telecommunications Sector Security Reforms.
[7] See Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022 (Cth).

(Carrier Licence Conditions – Security Information) Declaration 2022[8] was registered on 5 July 2022. This instrument requires carriers and eligible carriage service providers to notify the Australian Signals Directorate of cyber security incidents impacting applicable assets and report operational, control and interest information for each applicable asset to the Secretary of Home Affairs. These obligations overlap with broadly similar reporting obligations contained in the SOCI Act. To some extent, within this area of overlap in the telecommunications sector, the risk of duplication has been managed by 'turning on' obligations through existing sector-specific regulatory instruments, under the *Telecommunications Act 1997* (Cth), rather than under the SOCI Act.[9]

14. Another aspect of the overlap described above is the likelihood that responding to a cyber attack incident will engage multiple regulatory regimes which may impose divergent obligations. The Law Council has previously considered in detail the likely interaction between the reporting obligations under sections 30BC and 30BD of the SOCI Act, and the existing eligible data breach notification requirements under Part IIIC of the *Privacy Act 1988* (Cth) (**Privacy Act**).[10]

15. By way of illustration, a 'cyber security incident' that has a 'relevant impact' on an asset under the SOCI Act could involve the compromise of the confidentiality of personal information that is stored in the critical infrastructure asset, or that relates to the operation of the asset (such as client, customer, user or patient information) and is held by the APP entity for the purposes of the Privacy Act. Crucially, the Privacy Commissioner's assessment, investigation, complaints resolution and enforcement functions under Parts IV, V and VIB of the Privacy Act are also exercisable in relation to an eligible data breach, or potential breach.

Discussion Paper Questions

Core policy areas

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?

16. The Law Council considers the following critical areas, that were not canvassed in detail in the Discussion Paper, warrant further consideration in the Cyber Security Strategy:

- general principles of regulatory best practice to guide reform in this area;
- a review of government legislation that requires the retention of records by both government and businesses, with a view to whether that retention is warranted, and the duration of that retention; and
- less invasive alternatives to verify identity and minimise personal information held by private businesses.

[8] Minister for Communications, Telecommunications (Carrier Licence Conditions – Security Information) Declaration 2022 (5 July 2022).
[9] In relation to telecommunications sector, obligations have been implemented through the Telecommunications (Carrier Licence Conditions – Security Information) Declaration; Telecommunications (Carriage Service Provider – Security Information) Determination 2022.
[10] Law Council of Australia, Submission to Parliamentary Joint Committee on Intelligence and Security, Security Legislation Amendment (Critical Infrastructure) Bill 2020; and Review of the Security of Critical Infrastructure Act 2018 (Cth) (17 February 2021) 37-38.

General principles

17. The Cyber Security Strategy should stipulate a high-level commitment to ensuring any individual regulatory or legislative reform proposals are accompanied by comprehensive impact analysis to assist with informed evaluation by stakeholders. In this regard, impact statements should provide robust evidence addressing the following matters:[11]

    - policy makers should clearly demonstrate a public policy problem necessitating Australian Government intervention, and should examine a range of genuine and viable options, including non-regulatory options, to address the problem;
    - each proposal must include a clear set of objectives – these are used to select the best option and to shape evaluation;
    - regulation should not be the default option: the policy option offering the greatest net benefit for Australia — regulatory or non-regulatory — should always be the recommended option;
    - policy makers should consult in a genuine and timely way with affected businesses, community organisations and individuals, as well as other stakeholders, to ensure proposed changes deliver the best possible outcomes for Australia;
    - the information upon which policy makers base their decisions must be published at the earliest opportunity;
    - the most significant policy proposals must undergo a post-implementation review reflecting on the extent to which the stated objectives have been achieved to ensure settings remain focused on delivering the best possible outcomes for Australia.

18. Critically, impact analysis should occur in a holistic manner at the earliest opportunity to inform scrutiny of proposed regulatory or legislative changes. In this regard, the Law Council notes that stakeholders have experienced constraints in assessing previous tranches of cyber security reforms, including the progressive expansion and amendment to the Security of Critical Infrastructure regime. For instance, the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 deferred provision of regulatory impact statements to the release of sector specific statutory rules which would realise in greater detail the statutory regime.[12]

19. In this context, the Law Council observed the utility of stakeholders having access to as much information as possible about projected regulatory impacts and the way in which they are being considered, as part of the process of scrutinising the originating Bills, and not only when later examining subordinate legislation prescribing further details to make the regime operational.

20. Because of the fragmented development of cyber security standards highlighted above, regulatory impact statements should focus on ensuring new regulatory changes avoid the risk of duplication and overlap with existing norms. In cases

[11] Commonwealth of Australia, Department of Prime Minister and Cabinet, Office of Impact Analysis, Australian Government Guide to Policy Impact Analysis (March 2023).
[12] Law Council of Australia, Submission to Department of Home Affairs, Exposure Draft: Security Legislation Amendment (Critical Infrastructure) Bill 2020 (27 November 2020).

where overlap is unavoidable, for instance, where a particular cyber security incident triggers reporting obligations in relation to multiple regulatory agencies; the risk of confusion arising from an overlap can be ameliorated by consideration of a 'one-stop shop' for reporting cyber security incidents considered further below.

A review of legislation requiring retention of records

21. The Law Council considers that the Cyber Security Strategy should include a high-level commitment to a review of government legislation that require the retention of records by both government and businesses as to whether that retention is warranted and the duration of that retention. This is an important exercise that has already been proposed by the Government, in its Privacy Act Review Report,[13] as set out below.

22. In this regard, the Law Council supports Proposal 21.6 of the Privacy Act Review Report which proposes:[14]

> *The Commonwealth should undertake a review of all legal provisions that require 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.*

23. The Law Council endorses the objective of such a review being framed in this manner, noting the compelling need to keep personal information in certain circumstances (e.g., ID verification, anti-money laundering obligations, taxation).[15]

24. In conducting a review of legal provisions requiring retention of personal information, the Law Council reiterates its recommendation that the review include consideration of whether all records collected by the Commonwealth should legitimately be the subject of an exception to the privacy principles, including a right to erasure, as currently proposed. For instance, Australian Privacy Principle 11.2 requires APP entities to destroy or de-identify all personal information which they no longer need for any purpose for which the information may be lawfully used or disclosed under the Act. However, there are exceptions to this requirement, such as if the information is contained in a Commonwealth record[16] or the entity is required to retain the information by another Australian law or court order.[17] This exception arises both where the entity is an Australian Government agency, and where an entity has entered into a contract with an Australian Government agency.

Less invasive alternatives to verify identity

25. The Law Council notes that the ongoing development of Australia's Digital Identity legislation and Trusted Digital Identity Framework (**TDIF**) will have a significant bearing on cybersecurity. The Law Council has considered in detail the issues raised by the exposure draft of the Trusted Digital Identity Bill 2021.[18]

---

[13] Attorney General's Department, Privacy Act Review Report (2022), 13 Proposal 21.6. ('***Privacy Act Review Report'***)
[14] Ibid.
[15] Law Council of Australia, Submission to Attorney-General's Department, Government Response to the Privacy Act Review Report (13 April 2023).
[16] In general, a Commonwealth record (as defined in s 6 of the Privacy Act) can only be destroyed or altered in accordance with s 24 of the *Archives Act 1983* (Cth).
[17] Privacy Act Review Report, 225.
[18] Law Council of Australia, Submission to Digital Transformation Agency, Phase 3 of Australia's Digital Identity Legislation (28 October 2021).

26. The TDIF establishes a framework for the outsourcing of the identity verification process to accredited Australian businesses which offer digital identity services – where these accredited providers have access to an individual's personal information (e.g., biometric information) to authenticate that individual's digital identity. The Law Council reiterates its view that the establishment of digital identities is a highly sensitive proposal and must be implemented with careful consideration.

27. The Law Council acknowledges that the TDIF will provide considerable efficiency gains through the use of a secure and centralised accreditation system, particularly where the collection of information is limited to that which is absolutely necessary and proportionate safeguards are implemented, including the timely deletion of unnecessary information. However, the Law Council reiterates its view that participation in the TDIF should be voluntary and that non-digital systems for identity verification must also be maintained. The use of data under the TDIF must also be sufficiently transparent to enable users to provide informed consent, as well as withdraw enduring consent once it has been provided.[19]

28. The Law Council highlights that it is critical that future steps towards realising the TDIF in legislation should be subject to comprehensive consultation with stakeholders.

29. In addition to the framework envisaged in the TDIF, the Law Council encourages further consideration of other alternatives to alleviate the need for many private organisations to collect personal information in the first place being:

    - **token based authentication** – to tokenise existing digital verification services, providing individuals with a simpler way to authenticate their identity with entities. Token-based authentication allows users to verify their identity once using their personal information, and in return receive a unique access token (e.g., a string of random characters). This unique access token then serves as proof that a user has been authenticated. This would reduce the amount of identifying information required to be held by institutions;
    - **central identity verification platform or 'digital passport'** – for individual users to access services requiring identity verification, without businesses needing to store user data. If organisations were encouraged to avoid or prevented from storing sensitive or personal data, this would mitigate the impact of a data breach and would disincentivise criminal activity.

Enhancing and harmonising regulatory frameworks

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

Electronic funds transfer payment fraud

30. The electronic funds transfer (**EFT)** payment system relies solely on bank account numbers to facilitate the transfer of money between accounts. The legal profession and others are aware that there is a vulnerability in this system that can be exploited by criminals engaging in EFT payment fraud or cybercrime. This affects the legal profession as this vulnerability can be exploited through, amongst other cyberattack methods, business email compromise (**BEC**) scams.

[19] Ibid, 5 [4].

31. As part of the Cyber Security Strategy, the Australian Government should be actively considering the extent of its role in raising awareness, mitigating the impacts, and decreasing the occurrence of cyber-assisted fraud through BEC scams, noting that these types of scams are becoming prevalent across industries. In 2021, Australian businesses lost $227 million to BEC scams—an increase of 77 per cent since 2020.

32. While education and awareness activities will play a key role in responding to this growing issue, consideration should be given to further safeguards, including:

- the introduction of real-time name matching verification for EFT payments, noting that such initiatives have recently been implemented by several financial institutions; and

- consideration of how digitally signed emails with public key infrastructure authentication can be more widely adopted to help address this broader problem, which provides a trail to prove who created the signature, so recipients can verify the legitimacy of emails they receive.

33. The Law Council would welcome further consultation with relevant agencies on these matters.

The appropriate mechanism for reform

Question 2(a): What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy?

34. The Law Council has previously considered in detail the considerations bearing on assessing the appropriate mechanism for reform to improve cyber security standards across the economy.[20] In earlier submissions, the Law Council has suggested there are two critical considerations that should guide any effort to strengthen governance arrangements being:[21]

- **an impending need for cyber security agility** – as cyberattacks become increasingly sophisticated, there is an impending need to ensure cyber security practices can be regularly adapted and improved. Regulatory settings should provide incentives for Australian organisations to adopt a dynamic and iterative approach to assessment, mitigation and management of cyber security risks, that tracks and responds to emerging threats and vulnerabilities; and
- **defining the different roles of actors when managing cyber security risks across the supply chain** – mitigation and management of cyber security risks often require organisations to understand whether and how other entities are addressing security risks that arise within a multiparty data handling and processing ecosystem. Given the diversity of actors, increased complexity of supply chains for internet accessible devices and services, and the variety of contexts and scenarios of deployment and use, a 'one size fits all' regulatory requirement that a device or service must be 'secure' is unlikely to provide appropriate incentives for entities across a multiparty data handling and processing ecosystem to assess and address evolving cyber security risks.

[20] Law Council of Australia, Submission to Department of Home Affairs, Strengthening Australia's Cyber Security Regulations and Incentives (8 September 2021). (***'LCA 2021 Submission Strengthening Australia's Cyber Security Regulations'***)
[21] Ibid, 7 [15].

35. With that context in mind, the Law Council has generally favoured voluntary principles-based governance standards because it is the most agile and responsive approach to managing cyber security risk through corporate governance.[22] Such a standard should be developed in close consultation with the industry and then subject to broader public consultation.

36. It is noted that in other circumstances, voluntary standards for banking practices and climate reporting have been effective in providing a benchmark by which stakeholders can hold corporations and their boards to account for failing to comply with such standards. Significantly, a voluntary standard could be considered by a court when determining whether failures relating to the oversight of cyber risk constituted a breach of directors' duties.

Question 2(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?

37. In principle, the Law Council supports further consideration of expanding the definition of critical assets under the SOCI Act to include customer data, noting that the secure handling of this form of personal information is critical to the regular functioning of society, and is therefore, deserving of protection commensurate with other critical assets.

38. However, the Law Council supports more scrutiny of the unaddressed issues in relation to proportionality and certainty that have accompanied the expansion of the SOCI regime in recent years. These broader issues are discussed below.

39. The Security Legislation Amendment (Critical Infrastructure) Act 2021 (Cth), passed in December 2021, and the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (Cth), passed in March 2022, substantially expanded the scope of the existing critical infrastructure regime, under the SOCI Act, by focusing on cyber security threats to a far broader range of critical infrastructure assets (collectively these Acts are referred to as the **SOCI regime**).

40. The sectors regulated by the SOCI regime have been progressively expanded and now encompass a broad swathe of the economy including: communication, data storage, food and grocery, defence industry, energy, financial services, health care, higher education, space technology, transport and water.

41. Most relevantly, the recent December 2021 and March 2022 legislation established the following obligations:

- a requirement to notify cyber incidents impacting the critical infrastructure assets to the Australian Signals Directorate (in some cases, within 12 hours);
- a requirement to notify their data storage and processing service providers that they are managing 'business critical data';
- the possibility of Government assistance and intervention measures being taken, including a 'last resort' intervention request authorising the ASD to take positive actions to help defend the asset;
- a requirement to establish, maintain and comply with a written risk management program (with grace periods applying for some assets); and

[22] The Law Council, along with most of its Constituent Bodies supported voluntary principles-based regulation: LCA 2021 Submission Strengthening Australia's Cyber Security Regulations, 7-9. However, the Law Council also noted the contrary view of the Queensland Law Society: LCA 2021 Submission Strengthening Australia's Cyber Security Regulations, 10.

- an ability for the Government to declare certain critical infrastructure assets as being 'Systems of National Significance', entailing enhanced cyber security obligations, if required by the Secretary of Home Affairs, e.g. a need to develop incident response plans, providing access to system information and undertake cyber security exercises.

42. The Law Council considers that any expansion of the definition of critical asset should be preceded by a holistic review of the operation of the expanded SOCI regime by Parliament taking into account the views of stakeholders, with a particular focus on ensuring the regulatory burden imposed by the SOCI regime is proportionate and expressed in a clear and certain manner.

43. In this regard, the Law Council maintains support for amendments it recommended[23] to the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) inquiry, many of which were adopted by the PJCIS in it advisory report of September 2021.[24] The overarching objective of the Law Council's proposed amendments were directed to ensuring the SOCI regime contain safeguards which require the scheme to operate in a proportionate and accountable way, rather than this outcome being reliant on executive discretion.[25]

44. Critically, the Law Council maintains its long-held view that the extraordinary powers of Government intervention affecting private infrastructure, available under the SOCI regime, require independent, rather than Ministerial, authorisation.[26]

45. The Law Council reiterates its concern that the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* incompletely addressed the recommendations of the PJCIS.[27] The Law Council remains concerned about the unresolved and potentially counter-productive impacts of limitations in the scope of immunities extended to personnel and associates of regulated entities for acts done to comply with regulatory requirements.[28] Additionally, the Law Council remains concerned that there are limitations in the availability and effectiveness of review and oversight mechanisms for the expanded regulatory regime.[29]

46. In particular, the Law Council continues to advocate for a merits review system of appeal to the security division of the AAT with respect to declarations of critical infrastructure assets as systems of national significance and enhanced cyber security obligations for entities declared to be systems of national significance as recommended by the PJCIS.[30]

47. The Law Council supports further consideration, referring to the experience of stakeholders complying with the SOCI regime, of the potential overbreadth in

---

[23] Law Council of Australia, Submission to Parliamentary Joint Committee on Intelligence and Security, Security Legislation Amendment (Critical Infrastructure) Bill 2020; and Review of the Security of Critical Infrastructure Act 2018 (Cth) (17 February 2021). ('***Law Council PJCIS 2021 Submission***')
[24] Parliamentary Joint Committee on Intelligence and Security, Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018 (September 2021).
[25] Law Council PJCIS 2021 Submission, 6 [4]
[26] Ibid, 69-87.
[27] Law Council of Australia, Submission to the PJCIS, Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (2 February 2022). ('***Law Council PJCIS 2022 Submission***')
[28] The Law Council noted residual concerns, even after amendments, regarding scope of immunities in relation to contracted service providers to 'related companies' and actions of a regulated entity which are not clearly referable to one or more specific regulatory obligation under the SOCI Act: Law Council PJCIS 2022 Submission, 2-3 [7].
[29] Law Council PJCIS 2022 Submission, 4.
[30] Ibid 4 [8].

delegated legislative powers to prescribe an asset as a 'critical infrastructure asset' under the SOCI Act and its implications for proposed foreign investments in relation to those assets.[31] The Law Council has previously recommended that the next statutory review of the SOCI Act should include consideration of the implications of definitions in the SOCI Act for the *Foreign Investment Reform (Protecting Australia's National Security) Act 2020* (Cth).

48. Careful consideration must be given to potential overlap arising from the interaction between, an expanded SOCI Act, and the Privacy Act. The expansion of powers and safeguards under the SOCI Act should not undermine the ability of individuals to pursue their rights under the Privacy Act. Further information gathering and other powers, of the OAIC, designed to assist individuals should be preserved. Another key area of interaction between the SOCI regime and the Privacy Act, that must be considered further, is the legislative amendment of both Acts to explicitly specify how the reporting obligations for cyber security incidents under the SOCI regime will interact with data breach reporting requirements in Part IIIC of the Privacy Act. The Law Council has previously made detailed recommendations on this issue.[32]

Question 2(c): Should the obligations of company directors specifically address cyber security risks and consequences?

49. The primary concern with the introduction of further obligations on company directors is they may be too onerous and costly to comply with. There is a cumulative impact of a mandatory standard on the level of regulatory burden, and the high costs it would impose on businesses (which businesses would likely seek to pass onto consumers). Company directors are already subject to stringent regulatory requirements and face potential liability under a myriad of Commonwealth and state laws. The addition of further potential liability is undesirable. It would add complexity given the volatile nature of cyber risks without certainty of improved outcomes.

50. It is important to note that, even without a new obligation or governance standard, directors may incur liability for breaching the general directors' duties. In particular, company directors already are obliged by section 180 of the Corporations Act to manage their company with care and diligence. This obligation may be contravened if proper standards of cyber security are not implemented. The directors' duty of care and diligence could also be contravened if they fail to take appropriate steps to prevent contravention of cyber security laws, via 'stepping stones' liability under section 180 of the Corporations Act.

51. Additionally, if it appears that directors have turned a blind eye to data protection privacy requirements, the Australian Securities and Investments Commission (**ASIC**) may initiate an investigation. Serious cases, could lead to a pecuniary penalty, a compensation order, or disqualification of, directors.

52. It is likely that judicial expectations of what a reasonable director might do to manage cyber risk will rise due to the increasing awareness of cyber security risks, the increasing number of attacks and the potential damage. In short, section 180 of the Corporations Act provides an appropriate avenue to hold directors accountable.

53. Comparable international jurisdictions, Canada, the United States, the European Union and the United Kingdom, have not imposed a general duty on directors to

[31] Law Council PJCIS 2021 Submission, 34-36.
[32] Law Council PJCIS 2021 Submission, Recommendation 9, 9.

ensure the cyber security of their organisations.[33] Reliance has been placed on directors being subject to general duties of care, skill and diligence to their organisations. Crucially, in these jurisdictions, there is an increasing scope for actions to be brought directly against directors based on these general duties in relation to cyber security.[34]

A new Cyber Security Act

Question 2(d): Should Australia consider a Cyber Security Act, and what should this include?

54. At this stage, the Law Council does not consider there to be sufficient evidence to make an informed decision on the desirability of a consolidated Cyber Security Act. However, there are difficulties that would arise in relation to consolidation of cyber-specific legislative obligations and standards that require further consideration and consultation.

55. Despite this, the Law Council is not opposed to further consultation on the development of a Cyber Security Act. Any legislation must be supported by an appropriate enforcement and compliance regime and should include appropriate exemptions. If well pitched, a Cyber Security Act could be useful in providing a broad consolidation of regulatory norms and support harmonisation of Australia's privacy, data and cyber security regimes. It would also emphasise the need to mitigate the regulatory burden on affected entities caused by diffuse state and federal laws and regulations.

56. Regardless of whether a Cyber Security Act is introduced, the Privacy Act should remain the main legislative instrument relating to security measures for personal information. The Privacy Act primarily focuses on the various types of protected information and the circumstances in which such information may be used, collected or disclosed, instead of prescribing standards of protection. In contrast, a Cyber Security Act should be focussed on the general security profile of organisations.

57. Given the importance of ensuring prescribed standards referred to in legislation remain agile and responsive to changing technological circumstances, the Law Council notes that any legislation should preserve the ability of government to impose contemporaneous cyber security obligations predominantly through regulations and directions. Therefore, any Australian Cyber Security Act must be technologically neutral, flexible and responsive to deal with fast-paced developments in technology effectively.

58. For this reason, one focus of a Cyber Security Act may be to prescribe both minimum standards for cyber security for organisations, and the requirements for addressing cyber security (e.g., a requirement to implement multifactor authentication), to ensure Australia's approach to cyber security is uplifted.

59. The New South Wales Government, in collaboration with Standards Australia and AustCyber, recently considered the development of harmonised cyber security standards. The Law Council supports further consideration and consultation, at a national level, based on the findings of the NSW Cyber Security Standards Harmonisation Taskforce Recommendations Report (the **Recommendations Report**). The report identified seven priority areas for the development,

[33] King & Wood Mallesons, Report for the Australian Institute of Company Directors, International Comparison Cybersecurity Obligations (April 2023) 3 4.2.
[34] Ibid.

implementation and application of standards to build a resilient cyber infrastructure across sectors.

60. By way of example, the Recommendations Report supported the adoption of recognised International Organisation for Standardisation (**ISO**) or International Electrotechnical Commission (**IEC**) standards to outline baseline requirements for information security, protective security, and supply chain and risk management.

61. Additionally, the Recommendations Report cautioned against creating duplicative requirements at a cost to the business and broader community. It recommended any approach to cyber security standards should enable businesses to 'leverage their existing compliance or identify a maturity lift required from the baseline [requirements]'.[35]

62. The Law Society of New South Wales suggest that further consideration be given to the Australian Cyber Security Centre's 'Essential Eight Maturity Model' (**Essential Eight**). It is a useful and versatile framework for implementing more specific cyber security standards allowing for a context-sensitive approach to be taken in relation to the different actors across a supply chain.

63. As outlined above, given the importance of defining the different roles of actors when managing cyber security risks across the supply chain, an attractive feature of the Essential Eight model is the progressive distinction between maturity levels based on mitigating increasing levels of adversary tradecraft and targeting. In seeking to define more explicit cyber security obligations, consideration should be given to setting specific security standards based on both the type of entity involved, and the quantity and degree of sensitive data it holds. This is in accordance with the approach adopted under the Essential Eight model. It is also critical that the Essential Eight model be reviewed on an ongoing basis to ensure it remains fit for purpose, and if necessary, should be updated to broadly align with international standards.

64. The Law Council reiterates that consideration must be given to potential impacts of such legislation on various entities operating at different levels of the supply chain for the reasons outlined above.

65. In particular, the Law Council cautions against an approach that encourages regulated entities to simply shift their cyber security obligations onto third parties (such as technological infrastructure or cyber security providers). This may otherwise disincentivise providers from delivering certain important services, or markedly increase their prices to compensate for the additional regulatory risk.

66. Any proposed legislation must be mindful of the commercial relationships between businesses operating at multiple levels of the supply chain, including cyber security service providers, as well as the potential increase in overall costs of compliance.

67. In seeking to draw together cyber-specific legislative obligations and standards across industry and government, the Law Council suggests further clarification is required to clearly delineate the future roles and remit of the Australian Signals Directorate and Australian Cyber Security Centre.

[35] Ibid, 9.

Payment of ransoms

Question 2(f): Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals?

68. The Law Council reserves its position in relation to a prohibition on the payment of ransoms and extortion demands by victims of cyber attacks or insurers. Any , prohibition would be, to the Law Council's knowledge, a world-first and therefore must require detailed consideration. The Law Council urges consideration of the following matters which are not addressed in any detail in the Discussion Paper:

- An impact analysis that establishes the necessity for a prohibition and balances the benefits and costs of regulatory intervention;
- the detailed form a prohibition will take including the calibration of appropriate exceptions; and
- how a prohibition is to be implemented including phased implementation and iterative consultation with stakeholders.

69. The Law Council's Constituent Bodies hold differing views on the effectiveness of a prohibition in achieving its intended objective. The objective of a prohibition, identified in the Discussion Paper, is to 'help break the food chain,'[36] by removing the incentive for cyber criminals to engage in extortive behaviour, thereby, disrupting the business model of cyber criminals.

70. The Law Institute of Victoria supports reform which clarifies the law relating to payment of ransoms and extortion demands. Some members suggest it may be appropriate to legislate a prohibition on payment of ransoms and extortion demands, subject to limited exclusions including where there is an imminent threat to life or a critical asset. The Law Institute of Victoria suggests consideration of whether a specialised independent government panel could be instituted to determine whether a payment is permissible in the context of the cyber threat.[37]

71. However, the Queensland Law Society, while noting it does not have a final view on the efficacy of a prohibition, cautions that adopting a prohibition would be a world first and further evidence is required to substantiate the degree to which a prohibition in one jurisdiction will disrupt the global business model of cyber criminals.

72. It is important to note that other international jurisdictions have noted the difficulty in legislating a blanket prohibition against the payment of ransoms and extortion demands. In the United States, a taskforce convened by the Institute for Security and Technology has developed the 'Combating Ransomware – A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force' (**the Ransomware Framework**)[38] to provide support for American organisations wishing to prevent or respond to ransomware attacks.

73. The taskforce responsible for developing the Ransomware Framework did not reach consensus on prohibiting ransom payments but acknowledged that payments should be discouraged. The Ransomware Framework recommends three factors to

[36] Discussion Paper, 7.
[37] Australian Financial Review, Takeovers Panel model could help with $42b cyber crisis (afr.com) (29 August 2022).
[38] Institute for Security and Technology, Ransomware Taskforce, Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Taskforce (2021).

consider before prohibiting ransomware payments. The Law Council suggests that these three factors also merit further consideration in the Australian context:[39]

- allowing governments and organisations time to adapt to an abrupt change in law. This requires time-based milestones to allow for the implementation of victim support programs and appropriate insurance policies for private insurers;
- phasing in prohibitions in specific sectors over time. Prohibitions on ransomware payments could be applied to public entities before being extended to apply to the private sector; and
- establishing victim protection and support to offset the burden on victims and cover business continuity and remediation costs for organisations (e.g., establishing a Cyber Response and Recovery Fund which could be used to help cover business continuity and remediation costs for organizations attacked with ransomware; establish rapid response teams to assist life-line organizations (such as hospitals) to restore functionality quickly; and provide liability protection for business interruptions caused by refusing to pay ransoms).

74. If a prohibition against the payment of ransoms and extortion demands is adopted, it is critical that there be detailed consideration of appropriate exceptions. The Law Council is particularly concerned about circumstances where there is an imminent risk of harm which may outweigh the policy rationale for prohibition.

75. By way of illustration, the Law Council notes the potential for a cyberattack involving imminent risk of harm to a law firm's clients, client's personnel or contacts (arising from the attack upon the law firm) or the general public. In this regard, the Law Council notes the experience of the Queensland Law Society in encountering examples of cyberattacks where publishing stolen data would lead to immediate threat to life (e.g., in the case of negotiations in criminal matters) or great detriment to the clients concerned (e.g., counselling notes relating to historical child sex offences).

76. Consideration of appropriate exceptions from liability for contravening a prohibition on the payment of ransoms should also consider the professional obligations of solicitors and other regulated professions. For example, solicitors are subject to a paramount duty to the Court and the administration of justice which prevails to the extent of inconsistency with any other duty,[40] however, solicitors also owe a fundamental ethical duty to act in the best interests of a client in any matter in which the solicitor represents the client.[41] These obligations may also need to be evaluated against the threat of release of client information obtained in a ransomware attack. In this context, the Queensland Law Society's Ethics and Practice Centre has prepared a guidance note to the legal profession outlining how these ethical issues should be navigated.[42] These issues require further research and discussion.

77. The Law Council encourages further consideration of the current practices of insurers. The Law Institute of Victoria's members note that many insurers expressly prohibit the payment of ransoms or extortion demands from coverage under professional indemnity insurance policies, although organisations can obtain

[39] Ibid, 50.
[40] Law Council of Australia, Australian Solicitors Conduct Rules (24 August 2015) 3.1.
[41] Ibid, 4.1.1
[42] Queensland Law Society Ethics Centre, Is it Ethical (or legal) for law firms to pay cyber-ransom? (8 December 2017).

separate cyber insurance in the commercial market to provide them with their own insurable losses arising from cyber events.

Strengthening reporting and engagement after a cyber security incident

Question 8: During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate Australian Cyber Security Centre improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

78. In principle, the Law Council supports an explicit obligation of confidentiality upon the ASD/ACSC in order to incentivise timely reporting of cyber security incidents.

79. The Law Council recognises the countervailing public interest in ensuring that critical risk information is shared by the ASD/ACSC with regulators where clear breaches of legislative or regulatory standards have been identified. This incentivises organisations to comply with cyber security obligations. It is important that a general obligation of confidentiality be subject to precisely defined exceptions to allow for the enforcement of regulatory standards.

Question 9: Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

80. Currently, the Notifiable Data Breach (**NDB**) regime for notification of cyber security incidents is predicated on a 'serious harm' threshold, regardless of whether the incident is related to ransomware or extortion demands. The Law Council understands, many APP entities are notifying of data breaches out of an abundance of caution as soon as a data breach has become apparent and prior to seeking legal advice. This is done regardless of whether the data breach is 'likely to result in serious harm'.

81. Drawing on the practical experience of the NDB scheme which has been in operation now for over four years, the Law Council considers expanding the scope for voluntary notification a more effective means of increasing public understanding of cybercrime risks. This can be achieved by amending the NDB to enable an APP entity to notify the Office of the Australian Information Commissioner (**OAIC**) on a voluntary or preliminary basis, and then within an appropriate time period (reflective of how most matters require a sense of urgency and promptness), communicating with the OAIC whether the APP entity considers that data breach is one that is 'likely to result in serious harm'.[43] The Law Council considers a more informal, yet prompt, means of communication would provide an opportunity for transparency and collaboration, including early input of various parties, when a data breach becomes known.

82. The Law Council notes other views have been expressed in answer to this question. For instance, the Law Institute of Victoria's suggest that lowering the threshold for notification to ensure that cyber incidents are reported more generally may be more effective at improving the public understanding of the nature and scale of cybercrime activity. In considering this option further, it is critical that detailed impact analysis examine whether the compliance costs imposed by a lower mandatory threshold

[43] Law Council Privacy Submission, 80-84.

would be justified. The impact analysis should consider whether expanding the scope for voluntary reporting may be a less onerous alternative to achieve this objective.

Question 11: Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

83. There is a manifest need for legal professionals to increase their cyber skills and expertise, to counteract the evolving and increasingly sophisticated cyber security threats aimed at the legal profession. In addition to the government's proposed STEM agenda, the Law Council supports specific and targeted cyber skills on the basis of the increasing specialisation of knowledge in this area. In particular, the Law Council calls for further consideration of initiatives to encourage and incentivise professionals to upskill in cyber proficiency through the higher education system.

84. More broadly, consideration should be given to initiatives to develop and grow the cyber security workforce in Australia by supporting small businesses, and ensuring they are well placed to employ and, in turn, upskill the workforce.

Question 13: How should the government respond to major cyber incidents to protect Australians? Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

85. For the reasons outlined above, duplicative obligations that impose divergent reporting obligations increase the cost of compliance with no corresponding benefit in terms of cyber security protection and, additionally, produce uncertainty and confusion.

86. Critically, the establishment of a single reporting portal will alleviate some of the compliance costs associated with overlapping reporting obligations owed to multiple regulatory agencies. It will also allow these agencies to share information in relation to a critical cyber security incident in a timely manner.

87. Accordingly, the Law Council supports efforts to align reporting obligations across different sector specific regimes and the Security of Critical Infrastructure regime. In this regard, alignment of the following matters should be considered:

- who a report must be made to;
- the definition of the different categories of triggering cyber security incidents; and
- the time given to complying organisations to make a report.

88. Additionally, harmonisation of cyber security legislative and regulatory frameworks across Australian states and territories is essential to reduce complexity and minimise the cost of compliance for large multi-state entities. Simplification, clarity and prioritisation of reporting is key for reporting entities in responding to time critical incidents.

Supporting victims of cybercrime

Question 15: How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime? What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

89. In its response to the Privacy Act Review Report, the Law Council highlighted there is in-principle support for the proposed direct right of action and statutory tort for serious invasions of privacy. Views across the legal profession do though differ, and there are concerns as to its necessity and potential for unintended consequences.[44]

90. The Law Council looks forward to continuing consultation to ensure that there are no unintended consequences, for instance, ensure all causes of action, can be considered in context and that the creation of a right does not detract from the powers and resources afforded to the OAIC in its investigative and enforcement functions.

91. The Law Council notes that the direct right of action and a statutory tort for serious invasions of privacy will assist in providing victims of cybercrime with an avenue to seek compensation when their personal information has been subject to a data breach.

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?

92. The Law Council generally agrees a whole-of-government approach to cyber security is required. This will ensure government agencies at all levels are sufficiently funded to implement best practice strategies for compliance. Government departments and agencies demonstrating best practice will likely have a flow on effect for developing broader compliance strategies and improving knowledge bases across teams and organisations.

Evaluation measures

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

93. As a general principle, the Law Council notes evidence that prioritising data security and transparency improves confidence and utilisation of digital services. For instance, a recent PwC study found:

> *Overall, data security must remain a priority and citizens need to have confidence in the security measures taken. Citizens won't embrace services unless they're sure their data is secure. Almost 80% of citizens expect government to use and store personal data ethically and securely (and this rises to 90% for those who have high trust in government). But only 38% are more comfortable sharing their data online than attending government services in person and this has not improved over time (36% in June 2020).*[45]

[44] Law Council of Australia, Submission to Attorney-General's Department, Government response to the Privacy Act Review Report (13 April 2023) 37-40.
[45] PwC Australia, Bringing all citizens on the digital journey Citizen Survey 2022 (2022) 6.

94. The Law Council highlights the continuing importance of Freedom of Information processes being accessible, to ensure transparency in how government agencies are meeting their obligations and implementing cyber security strategies appropriately.

95. It is also essential that compulsory and regular reporting be a key feature of the Cyber Security Strategy.

96. The Law Council considers that the Cyber Security Strategy should lay down robust parameters, including independent oversight of government agencies in relation to progress against data security standards including the Protective Security Police Framework (**PSPF**).

97. For instance, a key limitation with assessing compliance against the PSPF is that the Attorney-General's Department, as the agency responsible for administering this policy, relies on self-assessment information provided by government agencies complying with the PSPF. Relevantly, the ANAO found:

> *AGD's advice to government about the progress of the framework was limited as AGD relied on self-assessment information, which the ANAO has found can be overstated or inaccurate, to accurately reflect the maturity of implementation of revised PSPF requirements. As policy owner, AGD did not monitor compliance with mandatory requirements. AGD provided a variety of support including detailed written guidance that could be better tailored to low-risk and face-to-face service environments. AGD's role can be strengthened by closer alignment of the self-assessment reporting instrument and policy, and by ensuring that entities understand and follow the mandated security reporting requirements*.[46]

98. The Law Council endorses these comments, and submits that the Cyber Security Strategy should reinforce the importance of agency accountability against data security obligations.

[46] Australian National Audit Office, Administration of the Revised Protective Security Policy Framework (12 May 2022) [10].