



Law Council
OF AUSTRALIA

Horizon 2 of the 2023–2030 Australian Cyber Security Strategy

Department of Home Affairs

8 September 2025

Telephone +61 2 6246 3788
Email mail@lawcouncil.au
PO Box 5350, Braddon ACT 2612
Level 1, MODE3, 24 Lonsdale Street,
Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.au

Table of contents

About the Law Council of Australia	3
Acknowledgements	4
Executive summary	5
Introduction	7
Particular challenges for small businesses	7
Small legal practices.....	8
Regulatory impact analysis for small business.....	8
Encouraging uptake.....	9
Unintended impacts for small business and the regions.....	9
Commentary on specific ‘cyber shields’	9
Shield 1: Strong businesses and citizens	10
Shield 4: Protected critical infrastructure	15
Shield 6: Strong region and global leadership	16

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; promotes and defends the rule of law; 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 107,000 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 2025 are:

- Ms Juliana Warner, President
- Ms Tania Wolff, President-elect
- Ms Elizabeth Shearer, Treasurer
- Mr Lachlan Molesworth, Executive Member
- Mr Justin Stewart-Ratray, Executive Member
- Mr Ante Golem, Executive Member

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

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

Acknowledgements

The Law Council of Australia acknowledges the contributions of the Law Institute of Victoria, Law Society of New South Wales, and Queensland Law Society in the preparation of this submission. We are also grateful for the assistance of the Law Council's Futures Committee and the Business Law Section's SME Business Law Committee.

Executive summary

The Law Council of Australia welcomes the opportunity to comment on Horizon 2 of the 2023–2030 Australian Cyber Security Strategy. In doing so, we continue to emphasise the need to ensure proportionality, consistency, and certainty within the regulatory landscape, while recognising the very real and potentially devastating impacts of cyber security threats.

The Law Council commends the Australian Government's speed in executing its Horizon 1 priorities during a crowded whole-of-government reform agenda. We were pleased to be actively involved in the development of a ransomware reporting framework and the rollout of various messaging and education campaigns.

Horizon 2 now represents an opportunity to embed cyber security messaging across society and empower businesses—especially small to medium businesses (**SMBs**)—to identify and proactively address cyber security risks.

Horizon 2 will be defined by its interaction with new developments in artificial intelligence (**AI**) and quantum technologies, and by how it aligns any developments with productivity outcomes. The fundamental challenge for the Australian Government will be to balance the tension between promoting regulatory and compliance obligations for businesses that are not unduly burdensome, whilst developing enhanced privacy and cyber security related outcomes for individuals and entities across Australia.

Given the significant detriment caused by cyberattacks and data breaches on individuals and organisations, including the costs incurred, cyber security management should no longer be considered optional. It is, therefore, critical that organisations of all sizes implement robust cyber security measures, supported by relevant minimum standards and codes. However, any such regulatory framework must be appropriately balanced so as not to unduly discourage innovation, and investment in innovation, in Australia.

In this submission, the Law Council highlights the specific challenges faced by SMBs in uplifting cyber security arrangements, with an emphasis on the unique circumstances of small legal practices. Key focus areas for the Law Council at this stage of the consultation are:

- the role of Horizon 2 in encouraging awareness of cyber security standards and providing a clear pathway for SMBs to understand what they may reasonably achieve with limited resources, coupled with implementation and targeted support;
- the benefits of a regulatory impact analysis with respect to any specific actions and initiatives relating to small businesses, to ensure the next stage of the Government's response adequately considers the impact on SMBs and allocation of sufficient government funding to support uptake and ongoing compliance;
- the growing profile of government and industry cyber security leaders deploying cyber security awareness and messaging, and the need for these voices to continue to be elevated across all levels of society; and
- the need for the Australian Government to support the private sector by ensuring consistency and education across public entities, especially among procurement officers and decision makers (not just its technical experts), so that there is a shared and consistent knowledge.

In addition, the Government should provide targeted grants, incentives, or subsidies to assist small businesses, including small legal practices, to encourage uptake of better cyber security practices. Without this support, small businesses risk being excluded from

Government contracts and partnerships with larger businesses, weakening regional economies and limiting national supply chain resilience.

The Law Council looks forward to continuing to engage with the Australian Government as it refines Australia's regulatory, legislative, and policy settings to build national cyber security resilience and enhance cyber security across the economy.

Introduction

1. The Law Council appreciates the opportunity to provide a submission to the Department of Home Affairs' Discussion Paper on Horizon 2 of the 2023–2030 Australian Cyber Security Strategy (**Horizon 2 Paper**).
2. We agree that a holistic and coordinated approach is needed to address what has become a key and endemic concern for all Australians due to the frequency and ubiquity of cyberattacks and data breaches across the public, private and other sectors. To this end, an effective cyber security strategy requires a coordinated response from all levels of government, particularly considering the significant social and economic costs associated with cyberattacks and data breaches.
3. The Law Council commends the Australian Government's speed in executing its Horizon 1 priorities during a crowded whole-of-government reform agenda. We were pleased to be actively involved in the development of a ransomware reporting framework and the rollout of various messaging and education campaigns.
4. Noting that Horizon 1 sought to strengthen the foundations of Australia's cyber security landscape, the Law Council believes Horizon 2 will be defined by its interaction with new developments in AI and quantum technologies, and in how to align any developments with productivity outcomes. The challenge for Government will be to balance the tension between promoting less burdensome regulatory and compliance obligations for businesses, whilst developing better privacy and cyber security related outcomes for society.
5. The Law Council continues to acknowledge and support the need for enhanced cyber security measures to safeguard both individuals and businesses that may be vulnerable to cyber threats. In addressing this need, we continue to emphasise that, while there is a need for an overarching framework for cyber security regulation, any regulatory framework must be appropriately balanced so as not to unduly discourage innovation and investment in Australia.

Particular challenges for small businesses

6. In implementing Horizon 2, support must be provided to small businesses that are increasingly under pressure to manage compliance and risks associated with cybercrime, privacy (and data security), and other reporting obligations.
7. The Australian Cyber Security Centre's (**ACSC's**) *Cyber security checklist for small businesses* recommends speaking to an information technology (**IT**) professional about securing networks and implementation of Maturity Level One of the 'Essential Eight' strategies to mitigate cyber security incidents.¹ However, resource constraints for small businesses will mean that, in many cases, those businesses will need to engage third parties to implement technical requirements, placing them at a disadvantage to those businesses with access to internal IT professionals.
8. While a maturity model approach is necessary when dealing with businesses with diverse threats and the resources to face them, the Essential Eight framework is not necessarily the most appropriate starting point for many smaller entities. It has a heavy focus on technical controls, including some that can be expensive to

¹ Australian Cyber Security Centre, *Cyber security checklist for small businesses* (June 2023) <<https://www.cyber.gov.au/sites/default/files/2023-06/Small%20business%20cyber%20security%20checklist.pdf>>.

implement. Other frameworks are emerging that may be a more suitable starting point for micro to small businesses.²

9. We note that the problem with regulatory responses of this kind is that, in contrast to a larger business, smaller businesses have fewer resources available to deal with increased regulatory burdens, running the risk of creating vertical inequity and resulting in economic distortions that would make SMBs less competitive in comparison to larger businesses.

Small legal practices

10. The challenge for legal businesses remains reconciling their unique vulnerability to cyber-crime (due to the sensitive personal information they hold) with limited resourcing and increasing (and potentially disproportionate) regulatory burdens. Over 90 percent of legal practices in Australia are small businesses of one to four principals,³ who are required to maintain large repositories of personal information due to data retention laws. These legal practices have limited capacity—in terms of finances and staff—to implement complex protection programs, unlike larger businesses with access to more resources.
11. In the Law Institute of Victoria's recent Legal Costs Benchmarking Survey,⁴ firms reported that four of the top 10 cost challenges for small law firms relate to cyber, data, IT security, and regulation. Consequently, small law practices (and small business generally) should remain at the forefront of Horizon 2 policy considerations. This is particularly pertinent, given that small legal practices already face growing regulatory burdens, such as the rollout of Tranche 2 of the Anti-Money Laundering and Counter Terrorism Financing (AML/CTF) regime, due to commence on 1 July 2026. In addition, small practices undertaking designated services under the *AML/CTF Act 2006* (Cth) will become subject to the requirements of the *Privacy Act 1988* (Cth) regime from the same date.⁵

Regulatory impact analysis for small business

12. In light of the above, the Australian Government must endeavour to control costs as regulation is increasingly applied to small businesses, including smaller legal practices. This is critical in a context where the financial impact on small businesses, as a result of cybercrime, continues to increase.
13. To mitigate potential vertical inequity and disproportionate allocation of regulatory burdens, we support a strengthened focus on providing small business clear and low-cost cyber standards, coupled with implementation and targeted support. We strongly suggest that these initiatives be co-designed with experts who have experience as owners of, and suppliers to, genuinely small businesses (including sole operators). This engagement should go beyond final stage consultation and

² Such as Dynamic Standards International's (DSI) SMB 1001.

³ Urbis, prepared for the Law Society of NSW, *2024 National Profile of Solicitors* (13 June 2025), <<https://www.lawsociety.com.au/sites/default/files/2025-06/2024%20National%20Profile%20of%20Solicitors%20-%20Final.pdf>> 28.

⁴ LIV Media, 'LIV releases report Benchmarking the Costs and Challenges of Practising Law in Victoria in 2025' Law Institute of Victoria (Media Release, 13 August 2025) <https://www.liv.asn.au/web/advocacy___media/web/advocacy/media_releases/2025/liv-releasesreport-benchmarking-the-costs-and-challenges-of-practising-law-in-victoria-in-2025.aspx>.

⁵ This is because many small legal practices are currently subject to the small business exemption under the Privacy Act. Legal practices who become 'reporting entities' for the purposes of the AML/CTF Act from 1 July 2026 will no longer be able to rely on the small business exemption for the activities carried on for the purposes of, or in connection with, activities relating to the AML regime: *Privacy Act 1988* (Cth) s 6E(1A).

should ensure that any regulation and guidance is designed from the ground up to be responsive to the needs of small business.

14. The Law Council would also welcome a regulatory impact analysis of any specific actions and initiatives that are proposed as part of this process. This would help to ensure that the next stage of the Government's response adequately considers the impact on small businesses and the allocation of sufficient Government funding to support uptake and ongoing compliance. The analysis should consider the impacts on small businesses of different sizes, types, and location.

Encouraging uptake

15. Safe harbour programs, free training, and low-cost certification should all be considered in preference to top-down regulation and shifting liability to small business.
16. Many small enterprises struggle to obtain expert assistance. This is because the cost of performing a gap analysis, educating the customer, then performing necessary work on a less-than-ideal network can be unattractive to providers who are already struggling with capacity to service existing clients. A well understood program that is provided 'in a box', and can be tailored to individual sectors, would lower the cost of delivery significantly.
17. Government support, through well-targeted grants or incentives, would be of significant assistance to smaller enterprises in addressing these issues and encouraging uptake of better cyber security practices.

Unintended impacts for small business and the regions

18. One of the unintended impacts of the current framework is that larger businesses are needing to carefully reconsider engaging with small businesses, due to third-party vendor risks.
19. It is further understood that procurement practices at a government level mean that small businesses, and those located in regional, rural, and remote (**RRR**) areas, are often ineligible to procure government contracts, as they simply do not have access to the necessary resources. Some areas will not have sufficient local capability in the IT sector. These impacts are more acute in RRR locations, meaning that fewer businesses in these areas will succeed in acquiring this work.
20. Accordingly, the Australian Government must also consider supporting small businesses, and those located in RRR areas, by subsidising programs they must participate in to meet any pre-qualification requirement to tender for government work.

Commentary on specific 'cyber shields'

21. The Horizon 2 Paper provides several questions relating to the six 'cyber shields' designed to safeguard Australian citizens and businesses. The Law Council's response is limited to Shield 1, Shield 4 and Shield 6, with reflections on each of these approaches set out below.

Shield 1: Strong businesses and citizens

Question 5: What could government do to better target and consolidate its cyber awareness message?

22. There is a growing profile of Government and industry cyber security leaders deploying cyber security awareness and messaging. The Law Council considers that the Australian Government should continue to elevate these voices.
23. In particular, we observe the increasing visibility of the Office of the Information Commissioner (**OAIC**) in the sector, which has led to greater recognition of the OAIC's work in the context of recent data breaches by telecommunications providers. However, the OIAC has well-publicised resource constraints. We are concerned that an ongoing failure to adequately resource the OAIC will adversely affect its ability to be at the forefront of public awareness and messaging.
24. The focus of existing cyber security messaging to date has largely been in the context of prevention efforts (e.g. how to recognise scams or suspicious activity, and how to adopt better practices to avoid data breaches). However, there is currently little visibility of the downstream effects of making a cybercrime report, or how an individual report results in better outcomes. The Australian Government should take the opportunity to more effectively communicate these outcomes to individuals who make reports.
25. In general, cyber awareness messaging from the Government is useful for setting expectations that:
 - cyber security should not be considered optional;
 - everyone needs to be cyber aware; and
 - no small business is too small to be a victim of cyberattacks.
26. In education materials, analogies may be drawn using easily understood images: for instance, that not having cyber security is akin to leaving one's front door open. Such materials should also be appropriately differentiated, having regard to the context and the typical level of digital and cyber literacy of the target audience. For example, messaging directed to technical IT professionals would be different to messaging for sales professionals.
27. More broadly, just as the Australian Government has an obligation to act as a model litigant, the Government should also endeavour to be a model in setting the 'gold standard' for cyber security. Given the growing number of online services storing Australians' personal and health information (including MyGov and My Health Record), the public's trust in the digital environment will be undermined if the Australian Government does not lead by example in its cyber security messaging and infrastructure.

Question 6: What programs or pilots have been successful in this context? What additional supports could be developed or scaled-up to address these issues in partnership with both education stakeholders and those with technical cyber security expertise?

28. Beyond the growing status of government and industry leaders like the OAIC, the 'Stop and Think' campaign appeared to be widespread and has added to the growing visibility of cyber security awareness.
29. From an industry context, the Law Council considers that the banking industry's online resources to address scams, fraud, and security alerts are an effective example of industry messaging. By way of example, the Commonwealth Bank have a scam, fraud and security alerts webpage that outlines how they contact their clients, advertises recent phishing attempts and their reporting function.⁶
30. The Horizon 2 Paper calls for a 'whole-of-economy and whole-of-nation approach',⁷ including making Australia a top destination for cyber security talent and a leader in cyber research.⁸ Noting this, the Australian Government could consider utilising various levers to attract and support cyber security professionals to work and live in Australia.

Question 7: How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?

31. The limited capacity of small businesses and not-for-profits (**NFPs**) means that their ability to use cyber resources depends on the complexity of the tools and programs. The Law Council believes that the most effective tools are those that take a simplified approach to risk mitigation, and ensure that businesses can take small steps with industry and Government assistance to achieve enhanced cyber resilience.
32. Government assistance is highly useful for small business to implement sophisticated requirements, such as digitising systems or conducting vulnerability assessments. Other jurisdictions, such as Hong Kong and Singapore, have established industry support schemes in this area. For example, in Hong Kong, services such as *Cybersec One*⁹ offer a model where businesses can apply for a free cyber security assessment and receive basic assistance. The scheme targets small and local primary schools, non-government organisations, and SMBs. Similarly, Singapore supports SMBs through its *Productivity Solutions Grant Cybersecurity Packages*,¹⁰ curating a list of pre-approved cyber security vendors and packages ideal for businesses without in-house expertise.

⁶ Commonwealth Bank, Latest scams, fraud and security alerts (Webpage, 5 August 2025) <<https://www.commbank.com.au/support/security/latest-scams-and-security-alerts.html>>.

⁷ Department of Home Affairs, Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy (2025) <<https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/charting-new-horizons-australian-cyber-security-strategy.pdf>> 1.

⁸ Ibid.

⁹ Hong Kong Internet Registration Corporation, CyberSec One (Webpage) <<https://cybersec.hkirc.hk/en/programme/cybersec-one>>.

¹⁰ Cyber Security Agency of Singapore, PSG Cybersecurity Solutions (Webpage, 12 February 2025) <<https://www.csa.gov.sg/our-programmes/support-for-enterprises/psg-cybersecurity-solutions>>.

33. The Law Council encourages the Australian Government to consider offering similar industry assistance. There may be cost synergies if the Government were to work with industry experts to offer free (or highly subsidised) assistance to small business.

Question 9: What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFPs?

34. If the Government invests resources into cyber security, industry will follow that example. For SMBs and NFPs, the Government should provide tailored materials, such as checklists, to alleviate the burden on volunteer boards. This is particularly important because of the large amount of personal information these organisations may hold.
35. We suggest, as a matter of best practice in relation to cyber security:
- that businesses align with the principles and guidelines outlined in the *Information Security Manual* developed by the Australian Signals Directorate and ACSC, as a baseline;
 - that businesses consider aligning their cyber security posture and standards to be equal to, or greater than, that of their most secure client—for example, clients who are regulated under the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**) or by the Australian Prudential Regulation Authority; and
 - where necessary, ensure that all suppliers (not just IT suppliers) understand the business’s cyber security standards and expectations.
36. There is scope to clarify what constitutes reasonable steps to uplift cyber security. As noted above, cyber security standards, such as the Dynamic Standards International SMB1001, may offer a structured approach to identifying and managing cyber security risks for SMBs, or the International Organisation for Standardisation standards for more mature organisations.
37. Horizon 2 should focus on encouraging awareness of cyber security standards and provide a clear pathway for small business and NFPs to understand what level of cyber resilience they may reasonably achieve with limited resources, and how they can achieve this.
38. As noted above, many of the cyber security standards that are promoted by the Government (particularly the Essential Eight) can be technical in nature, to the extent that small business owners are often discouraged from engaging with cyber security. There must be a greater emphasis on education, engagement, and support for small business to encourage and incentivise cyber security compliance.
39. While various supports are already in place, including the Cyber Wardens free online cyber security training program for small businesses,¹¹ further assistance is required to directly promote cyber security for businesses that do not directly engage with technology. As raised above, the Government should consider offering subsidies or incentives to SMBs to support their increased uptake of better practice cyber resilience strategies. Funding could also be made available for cyber security experts to directly engage with small business operators.

¹¹ See, <<https://train.cyberwardens.com.au/>>.

40. In addition, Government engagement with national and State/Territory professional bodies would increase visibility of the issues and boost engagement across industries.

Question 10: What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?

41. Resourcing remains the largest issue. Small NFPs lack the labour and financial resources to engage with sophisticated cyber security resources, and often have unique and less formal (and therefore more complex) operating models.
42. In the Law Council's view, Australian Government assistance, for example through industry partnered programs as seen in Singapore and Hong Kong, would greatly assist small business and NFPs to enhance their cyber security.

Question 11: Do you consider cyber insurance products to be affordable and accessible, particularly for small entities? If not, what factors are holding back uptake of cyber insurance?

43. Cyber insurance products can be expensive and inaccessible for SMBs. At present, business coverage rates in Australia are likely slowed by a perceived lack of effective data security, owing to factors such as inconsistent skills and staff retention, advanced social engineering by attackers, and changing security ecosystems from hybrid work arrangements. SMBs in particular do not often have the security controls in place that insurance companies may require to mitigate these risk factors.
44. As clarity around compliance standards and the accessibility of industry-partnered cyber assistance programs improve, insurers will be able to more easily assess whether a business has taken reasonable steps to achieve a high standard of security, and measure the degree of risk associated with insurance assessments. It is likely that, in time, the cost of insurance premiums will decrease as the pool of historical data enables insurers to have more methodological sophistication in their risk and cost assessment tools.
45. Improving the confidence of insurers to engage with small businesses should be a priority for the Australian Government in the delivery of Horizon 2.

Questions 12/13: How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing? How could the government further support businesses and individuals to protect themselves from ransomware attacks?

46. The *Annual Cyber Threat Report 2023–2024*, published by the Australian Signals Directorate (ASD), states that 11 per cent of all incidents ASD responded to included ransomware (representing a three percent increase from the previous financial year).¹²
47. Anecdotally, members of the profession report that there appears to be a slight decrease in sophisticated ransomware incidents in the Australian context. Feedback to the Law Council suggests that where ransomware attacks occur, the

¹² Australian Signals Directorate, *Annual Cyber Threat Report 2023-2024* (November 2024) <<https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024>> 13.

attacker no longer appears focussed on holding data systems 'hostage'. Rather, the attacker appears geared towards exfiltrating data for commercial purposes.

Question 14: Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector? If so, what were the vulnerabilities and impacts that your community faced?

48. We reiterate that small legal practices are both uniquely vulnerable to cyber security risks and currently face greater regulatory burden with the rollout of Tranche 2 of the AML/CTF regime. The nature of the work conducted by legal professionals requires that practices hold sensitive personal information for extended periods of time due to conflicting privacy and data retention obligations. A significant portion of solicitors across Australia work in small businesses or as sole practitioners, meaning that they have limited capacity to develop sophisticated cyber security infrastructure.

Question 16: Which regulations do you consider most important in reducing overall cyber risk in Australia?

49. We suggest that regulation that protects data and compels behaviour must be easy to understand and comply with, and that it should contain meaningful enforcement or penalty mechanisms.
50. Arguably, the OAIC has taken a step in this direction with the Australian Information Commissioner's Notice of Filing in the Federal Court of Australia against Medibank Private,¹³ and its broad recommendations regarding minimum standards for larger organisations.¹⁴
51. We note that there is no general duty for a company to implement cyber security or data protection systems under Australia's corporations legislation. However, Australian Financial Services Licence (AFSL) holders are 'required by law to have adequate cyber security risk management systems in place',¹⁵ and the Australian Securities and Investments Commission has been actively litigating against AFSL holders for cyber security failings.¹⁶ APRA-regulated entities are also subject to specific data protection obligations.¹⁷
52. We query why only limited categories of entities are held to this standard, despite other industries holding substantial amounts of data and personal information, and often with fewer resources to protect that information.

¹³ Federal Court of Australia, Notice of Filing, Australian Information Commissioner v Medibank Private Limited (2024) <https://www.oaic.gov.au/__data/assets/pdf_file/0025/221974/Australian-Information-Commissioner-v-Medibank-Private-Limited-concise-statement.pdf>.

¹⁴ Ibid, Annexure B.

¹⁵ See, for example, comments by ASIC Chair Joe Longo in ASIC Media Release, 13 March 2025: <https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2025-releases/25-035mr-asic-sues-fiig-securitiesfor-systemic-and-prolonged-cybersecurity-failures/>.

¹⁶ See, for example, *ASIC v RI Advice Group Pty Ltd* [2021] FCA 1193; *ASIC v Fortnum Private Wealth Ltd* (2025); *ASIC v FIIG Securities Limited* (2025).

¹⁷ Refer to Prudential Standard CPS 234: Information Security: 'This Prudential Standard aims to ensure that an APRA regulated entity takes measures to be resilient against information security incidents (including cyberattacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats.'

Question 17: Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?

53. Legal practitioners are subject to data retention obligations, including an obligation to retain client documents and files for a period of seven years. Client files may be destroyed after this period, except where a client indicates otherwise, or where legal obligations exist to the contrary.
54. Notably, certain hard documents should never be destroyed, including documents of 'evidentiary value including original wills, will instructions, sealed court orders, original hard copy agreements or contracts'¹⁸ as well as deeds, adoption papers, leases, binding financial agreements, and other original documents that may be the subject of litigation. Data retention obligations can also extend beyond this legislative period in certain circumstances.
55. These requirements result in a growing pool of sensitive information held by legal practices which increases the potential magnitude of a cyber security incident. These data retention obligations are not necessarily 'negative', but they add a layer of vulnerability for small legal practices in the context of cyber security crimes.

Shield 4: Protected critical infrastructure

Question 35: Is the regulatory burden on industry proportionate to the risk and outcomes being sought?

56. Feedback received suggests that the regulatory burden for reporting often proves too onerous or rigid for organisations during a cyber breach, where quick and agile responses are required.
57. The varied layers of reporting obligations under the SOCI Act, Privacy Act, and other legislation can prove complex and costly for organisations, and even more burdensome for organisations that also have international reporting obligations. Instead of concentrating their resources on quickly responding to the breach, an entity's resources are often diverted to understanding and navigating the regulatory landscape.

Question 36: What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?

58. We suggest implementing regular audits of critical infrastructure to motivate best practice. For example, a 'cyber drill' may be very beneficial in identifying the strengths and weaknesses in the infrastructure by simulating a cyber-attack. To further incentivise organisations, we suggest considering the policy option of reducing insurance premiums if cyber drills are performed at regular intervals.

¹⁸ See Victorian Legal Services Board and Commissioner, Going Digital: Record-keeping guidance (June 2023) <<https://lsbc.vic.gov.au/lawyers/practising-law/running-law-practice/going-digital-record-keeping-guidance>>.

Question 37: How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?

59. The Australian Government could support the private sector by ensuring consistency and education across public entities, especially among procurement officers and decision makers (not just its technical experts), so that there is a shared and consistent knowledge.
60. When supplying goods or services to Government, businesses may face the challenge of inconsistent positions between Departments. Further, businesses may sometimes have a better understanding of the technical security requirements, certifications, and controls than the Government's representatives. This not only leads to substantial waste in the contracting process, but also leads to misaligned or poorly scoped projects, or projects with compliance costs that were unnecessary (for example, because a procurement officer did not understand which of the default standards included in the Government's template contracts could be safely removed).
61. In our view, the Government should also ensure that, when selecting suppliers for any of its Panels (including for its legal services, technical services, or other professional consulting panels), it should test panel applicants for their understanding of Government Frameworks, rather than simply requiring contractual compliance on paper. Members of the legal profession have observed that it is routine for Government to include a 'shopping list' of standards and controls (for example, the default terms for the Government's Digital Marketplace Panels), but that these can be treated as a box-ticking exercise, with no real validation undertaken.
62. Simultaneously, the Government can continue supporting the work of the ASD in terms of thought leadership and guidance, so that businesses are encouraged to align to a national standard. The Protective Security Policy Framework (**PSPF**) provides a good framework and, in the absence of any other national framework, may be the best option for Australian businesses to align to. However, not all businesses will have the resources, time, or technical expertise to comply with the PSPF.

Shield 6: Strong region and global leadership

Question 46: Do you view attributions, advisories and sanctions effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?

63. We acknowledge that, while sanctions might be effective tools against state actors, many malicious cyber actors will not be affected by such, or their commercial gain from such activities far outweighs any detriment. This is especially the case if they are never identified by name, or they belong to a State that Australia has already sanctioned, and are therefore unconcerned about further sanctions.
64. In some cases, attributions are more likely to be considered as 'status' points for threat actors, and are likely to encourage this unwanted behaviour. We understand that many threat actors trade on a reputation built on attributions for their past activities.

65. Information sharing and advisories can assist if they are informative, have clear action items, and are gazetted to persons who should know (or otherwise, if there is a method for such persons to subscribe to).
66. In our view, cyber diplomacy as a concept is unlikely to be useful. As above, where a threat actor is taking such actions because they are either taking directions from a State or they have a vested commercial interest, there is little 'diplomacy' to be had. From a pragmatic perspective, Australia needs to uplift its practices across business, government, and community to be less of a target; and equally, it may need to consider what national-level responses it should take if being attacked by another nation State.
67. As a non-hostile deterrence, the Australian Government could institute standards for data redundancy (i.e. enshrining best practice for data redundancy in law). Many ransomware events are perceived threats due to the loss of the compromised data, in addition to the potential release or exposure of it. However, if data loss is mitigated or entirely avoided due to enforced data backups, then this would decrease the level of concern for those involved. It is likely that by enshrining data redundancy measures in law, insurers would also follow suit. While this may have a cost impact on business, it would likely lead to a discernible shift in practice.

Question 47: Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?

68. We suggest uplifting domestic capability in cyber security. We also suggest that the Government continues to support the work of the Department of Foreign Affairs and Trade in the Pacific and with the countries in the Association of Southeast Asian Nations in continuing to develop cyber security legislation and supporting hard infrastructure.¹⁹

¹⁹ Department of Foreign Affairs and Trade, 'Pacific Cyber Security Operational Network': <https://www.dfat.gov.au/international-relations/themes/cyber-affairs/cyber-cooperation-program/pacific-cyber-securityoperational-network-pacson>.