Law Council
OF AUSTRALIA

20 July 2026

Ms Susheila Vijendran
Chair
Australian Registrars' National Electronic Conveyancing Council

By email: chair@arnecc.gov.au

Dear Ms Vijendran

Model Operating Requirements and Model Participation Rules—
Version 8 Consultation Drafts

1. The Law Council of Australia appreciates the opportunity to provide a submission to the Australian Registrars' National Electronic Conveyancing Council (**ARNECC**) about the Version 8 Consultation Drafts of the Model Operating Requirements (**MORs**) and Model Participation Rules (**MPRs**).

2. We thank the Law Society of New South Wales, the Queensland Law Society and the Law Council's National Electronic Conveyancing System Committee for their contributions to the preparation of this submission.

3. The Law Council is generally supportive of the steps taken by ARNECC to identify opportunities to improve the cyber security governance arrangements of Electronic Lodgment Network Operators (**ELNOs**) under the MORs and Subscribers under the MPRs. We recognise the changes are intended to improve security for users and consumers.

4. However, we make the following specific comments in relation to the draft MPRs.

Rule 2.1—Definitions

Cyber Security Framework

5. The proposed definition of "Cyber Security Framework" under Rule 2.1 has been introduced in conjunction with proposed Rule 7.11(b) (Secure use of systems) and states:

> ***Cyber Security Framework*** *means:*
>
> *(a) Essential Eight developed by the Australian Signals Directorate; or*
>
> *(b) ISO Standard 27001 developed by the International Organisation for Standardisation; or*
>
> *(c) SMB 1001 developed by Dynamic Standards International; or*

(d) *if any of the above is superseded, the cyber security framework that has superseded it, or such other alternative cyber security framework as is substantially equivalent to that Cyber Security Framework.*

6. We support the flexibility inherent in the definition provided, as the three standards identified focus on different areas, with differing costs of compliance. For example, in our view, ISO Standard 27001 requires the greatest cost and effort to achieve. While we understand that some larger law firms have achieved certification under ISO 27001, the costs of compliance with this standard are likely to be out of reach for smaller practices. Conversely, SMB-1001 may be more appropriate for small to medium law firms, as it sets a standard that is appropriate and achievable for these businesses.

7. However, more precision in describing the elements of a particular standard that must be met for a Subscriber to discharge their obligations under proposed Rule 7.11 would be beneficial. For example, SMB 1001 consists of 5 levels of increasingly advanced security measures requiring increasingly complex degrees of audit and validation protocols. As drafted, if a Subscriber chose to deploy SMB 1001 pursuant to proposed Rule 7.11(b)(i), there is no guidance about which level of that standard must be complied with.

8. We note that the Essential Eight (**E8**) framework could serve as a useful 'baseline' standard. However, as the Australian Signals Directorate (**ASD**) does not conduct any assessment or certification for organisations against the E8, firms adopting that standard would need to obtain independent certification from reputable E8 assessors to ensure and demonstrate their compliance, both for the benefit of the Subscriber's clients and to engage the 'safe harbour' provisions under the draft MPRs. That would entail organisations committing additional time and resources, including the significant costs of certification assessments and any remedial action required to address any identified non-compliance.

9. Consideration could also be given to including the Information Security Manual (**ISM**),[1] developed by the ASD, as another framework in the definition of "Cyber Security Framework". The ISM, which incorporates the E8 as a baseline and is a more detailed standard, is currently a requirement that organisations must meet as part of supplying certain services to government.[2] This involves an independent assessment of an organisation's security posture under the Infosec Registered Assessors Program.[3]

---

1 Australian Signals Directorate, Information security manual (June 2026).

2 For example, see the commentary on Information security and cyber security published by the Australian Government: Department of Finance, Selling to Government – Security requirements (Web Page).

3 Australian Signals Directorate, Infosec Registered Assessors Program (IRAP) (Web Page, 17 November 2025).

Jeopardised Conveyancing Transaction

10. The definition of "Jeopardised Conveyancing Transaction" is proposed to be revised to mean:

> *… a Conveyancing Transaction which has put, is putting or could put at risk the integrity of the Titles Register because of fraud or other means.*

11. This definition is unduly broad and open to subjective interpretation. The inclusion of Conveyancing Transactions which "could" put at risk the integrity of the Titles Register should be removed from the proposed revised definition. The replacement of "could" with "would" may be preferable.

Personal Information

12. The definition of "Personal Information" is proposed to be revised to mean:

> *… has the meaning given to it in the Privacy Act 1988 (Cth) and any State or Territory privacy legislation.*

13. Instead of the new words "any State or Territory privacy legislation", we suggest that, for clarity and consistency, the language should mirror the approach taken in Rule 6.7 and reference the privacy legislation for the Jurisdiction in which the land the subject of the Conveyancing Transaction is situated.

Subscriber Systems

14. The current definition of Subscriber Systems is:

> *… the information technology systems (both hardware and software) used by the Subscriber.*

15. This definition is not proposed to be amended in the draft MPRs. However, given the expanded role that this definition will play as a result of the proposed amendments, we submit that the definition must now be more circumscribed.

16. A law firm will operate numerous systems, many of which will not have any relevance or connection to the undertaking of a Conveyancing Transaction (for example, a litigation management system or an accounting system). It would be highly inappropriate for the MPRs to have general application to all systems of a law firm Subscriber, which may be an unintended consequence of the original broad drafting.

17. We recommend that the definition of "Subscriber Systems" be expressly limited to systems used "to implement the Subscriber's interaction with an ELNO as part of a Conveyancing Transaction".

Rule 6.3—Client Authorisation

18. Proposed amendments to Rule 6.3 would remove the exemption for the provision of a Client Authorisation for caveats, priority notices, extensions of priority notices and withdrawals of priority notices. The Explanatory Notes advise that this amendment has been proposed because "[t]echnological advances mean that obtaining an urgent Client Authorisation for a Caveat or Priority Notice is now possible".[4]

19. Although removal of the exemption in relation to priority notices and their extension or withdrawal is feasible, we oppose the exemption being removed for caveats. By their very nature caveats are time sensitive. The position of those with a legitimate interest may be jeopardised by any delay caused by needing to obtain a Client Authorisation, notwithstanding any possible acceleration of that process by reason of technological advancements. Depending on an individual Client's circumstances, it may not be possible to take advantage of those advancements in every case where an urgent Client Authorisation is required. Delays in obtaining Client Authorisations are also often attributable to the actual unavailability of the Client and the ability of technology to overcome this issue is limited.

20. We therefore recommend that the current exemption from obtaining a Client Authorisation should be preserved for Caveats, and that proposed Rule 6.3, and the definition of "Client" in proposed Rule 2.1, be revised accordingly.

Rule 7.1—Protection measures

21. We have significant concerns in respect of proposed Rule 7.1(d), which introduces a new Subscriber obligation to take reasonable steps to implement multi-factor authentication (**MFA**) for all Users in three contexts:

    (i) remote access (including virtual private network access) of the Subscriber's Systems;

    (ii) access to the account of a Subscriber Administrator; and

    (iii) use of email accounts.

22. In our view, the breadth of Rule 7.1(d) makes it unworkable. In the case of a law firm, it would appear to require implementation of MFA across the entire firm, including in areas that have no connection to eConveyancing. For example, proposed Rule 7.1(d)(i), which seeks to mandate the use of MFA for all remote access of the Subscriber's Systems, would require the use of MFA for remote access by all of the law firm's staff, including non-lawyers.

23. In larger firms, most staff would not be involved in eConveyancing. For smaller firms, the implementation and compliance burden may be too onerous relative to any security benefit to be derived. There is also no direct link from a Subscriber's email account to an Electronic Lodgment Network (**ELN**), and any of the email notifications from the ELN contain de-identified data only. While certain law firm systems, including email accounts, may indirectly support the eConveyancing process, it is not appropriate, in our view, for ARNECC to seek to regulate the operation of law firms and law firm systems in this manner. For this reason, we oppose proposed Rule 7.1(d).

---

4 ARNECC, Model Participation Rules (MPR) Consultation Draft 8.01 – Explanatory Notes (May 2026) 2.

24. We also query the utility of proposed Rule 7.1(d)(ii), noting that both PEXA and Sympli stipulate the use of MFA to access their respective ELNs. For example, under clause 5 of the PEXA Subscriber Security Policy, all Users are required to use MFA to access the PEXA System or perform certain actions within it.[5] Similarly, under clause 5.3.7 of the Sympli Subscriber Security Policy, access to the Sympli ELN requires the use of MFA.[6] In our view, this is an appropriately targeted requirement for MFA in the eConveyancing ecosystem, and no broader requirement for MFA should be mandated. Consideration could instead be given to amending the MORs to mandate that ELNOs require their Subscribers to use MFA to access the ELN. That would embed the current practice as a regulatory requirement. In our view, this would be a realistic and fairly targeted use of MFA in maintaining the security of the eConveyancing system overall.

25. There are varying degrees of adoption of MFA in law firms already, but the implementation costs and compliance burden of stipulating MFA as proposed is too onerous for smaller firms. Further, MFA implementation is a binary proposition: it is either implemented, or it is not. While the language of "reasonable steps" might, at least superficially, soften the proposed mandate, it is unclear to us how a reasonable steps approach could work in this context. We acknowledge the benefits of MFA, and support law firms choosing to adopt MFA, but it is not appropriate, in our view, for ARNECC to mandate the specific use of MFA as proposed. Accordingly, we request that Rule 7.1(d) be deleted. If proposed Rule 7.1(d) is to be implemented, we request a longer lead time to enable law firms to prepare. This date should be at least 12 months from the finalisation and publication of Version 8 of the MPRs.

Rule 7.11—Secure use of systems

26. Proposed Rule 7.11 establishes a new Subscriber obligation to take reasonable steps to ensure secure use of certain systems and provides a safe harbour for Subscribers who obtain annual certification under specified cyber security frameworks. We generally support proposed Rule 7.11 and the flexibility it provides, which is important due to the varied size, nature, location and resources of law firms.

27. As there will also be variation among law firms as to their current cyber security posture, we suggest it would be appropriate to provide a longer lead time to facilitate education and preparation, including implementing the necessary system controls and obtaining certification where that is the approach chosen by the Subscriber. We suggest that the lead time should be at least 12 months from the finalisation and publication of Version 8 of the MPRs. Providing a clear commencement date for Rule 7.11 will also assist with the interpretation of proposed Rule 7.11(b) and the timeframe within which Subscribers must obtain certification.

28. In relation to proposed Rule 7.11(a)(iv), in addition to deleting the redundant words "use of", the reference to email accounts should be confined to the Subscriber's email accounts used in the conduct of a Conveyancing Transaction.

---

5 PEXA, PEXA Subscriber Security Policy (Version 4, 5 August 2025, effective from 9 October 2025).
6 Sympli, Subscriber Security Policy (Version 6, March 2026).

29. Should the proposed changes proceed, we suggest that Model Participation Rules Guidance Note 8 "System Security & Integrity" be updated.[7] In connection with proposed Rule 7.11, the Guidance Note should be expanded to include:

    - Examples of the factors that may be considered in relation to the obligation to take reasonable steps under proposed Rule 7.11(a).
    - Introductory information about the cyber security standards that are referenced in the definition of a "Cyber Security Framework".
    - Commentary on the effect of not maintaining annual certification under proposed Rule 7.11(b)(i). There may be cases where certification is sought but not obtained. In those instances, it may be possible to establish compliance with the threshold of reasonable steps, but this would be a matter to be determined in all the circumstances.
    - Commentary about evidencing annual certification as compliant with a Cyber Security Framework. For example, we understand that ISO 27001 audits are undertaken by accredited third party assessors who issue a certificate.

30. We also note that Model Participation Rules Guidance Note 6 "Compliance Examinations" will likely need to be updated.[8]

Schedule 6—Insurance Rules

31. The Law Council is particularly concerned about the workability of the proposed reforms to the Insurance Rules,[9] and would welcome the opportunity to meet with ARNECC representatives to discuss these reforms before they are implemented.

32. We refer below to the numbering in MPRs Consultation Draft 8, but note that there appears to be an error in the numbering of Schedule 6 as a result of the provisions starting with Rule 0 rather than Rule 1.

Rule 0.3(f)

33. We note that Insurance Rule 0.3(f) requires coverage to be extended to:

> *… any dishonest, fraudulent, criminal or malicious act or omission by the Subscriber or the Subscriber's principals, Officers or employees in connection with Conveyancing Transactions.*

34. Generally, a standard professional indemnity insurance policy would not provide such cover, so Subscribers will have difficulty obtaining the required extended coverage. This is not directly relevant for Subscriber law firms that would generally be relying on the deeming provision in Insurance Rule 3.1(a) but will be relevant for other Subscribers.

---

7 ARNECC, Model Participation Rules Guidance Note 8 – System Security & Integrity (August 2024).
8 ARNECC, Model Participation Rules Guidance Note 6 – Compliance Examinations (August 2024).
9 See also, Law Council of Australia, Submission to ARNECC, Cyber security risks in the eConveyancing landscape: legal practitioner insurance requirements (16 April 2026).

35. We have serious concerns with Insurance Rule 0.5, and the requirements for specific cover for cyber security insurance for enterprise risks, including cover for incident response, business interruption and data/system recovery (first party claims) as well as third party claims arising from cyber incidents. We query whether ARNECC has considered the current and ongoing availability of cyber security insurance that will meet the requirements of Insurance Rule 0.5. The requisite market analysis for that purpose should include matters of product availability (that is, to what extent the products exist and whether they would continue to exist, as a compulsory requirement for cyber insurance could significantly change the underwriting risk profile for this market), as well as the future of premiums.

36. This significant change in the MPRs may create an unexpected need for new insurance. In the absence of an analysis of the market's capacity to provide such insurance, the proposed requirement may, if enforced on its current terms, create a sudden loss of Subscribers.

37. The Law Council understands that Lawcover's professional indemnity insurance policy, which is held by most legal practices in NSW, the ACT and the NT, provides third party cover up to a limit of $2 million at minimum.[10] It does not respond directly to cyber acts or incidents, but may provide third party cover in some circumstances, such as some cases of business email compromise. Additionally, cyber security cover is currently broadly available through Lawcover's cyber risk policy,[11] which provides all of its insured law practices with access to cover through a group cyber risk policy providing first party cover for losses arising from cyber incidents. That cover is limited to $50,000 annually per claim and in the aggregate.

38. Although some cyber risk policies (such as Lawcover's policy) provide limited coverage, we do not support mandating cyber security insurance for enterprise risks (including incident response, business interruption and data/system recovery). This requirement may be particularly problematic if insurers adjust or discontinue their policies in the future.

39. First party business risks and insurance are a much broader issue for legal practices and other Subscribers. The nature and extent of insurance for first party risks, including cyber risk, is more appropriately determined by each Subscriber having regard to the size and nature of its business. In our view, it is not appropriate for the MPRs to effectively require law firms to take out specific first party cover for cyber risk. Accordingly, we are unable to support the inclusion of Insurance Rule 0.5 as drafted.

40. We note that the changes proposed under Rule 0.5 will mandate specific levels of cyber insurance coverage. This specificity raises the following potential issues:

    (a) Practitioners will be subject to the unilateral decisions of ARNECC about what monetary amount will qualify as appropriate insurance cover for their business, which is an inappropriate 'one size fits all' approach. As discussed above, we consider that each individual law firm is best placed to determine what insurance cover is appropriate and adequate for its particular business and subsequent risk assessment.

---

[10] Lawcover, Professional Indemnity Insurance (PII) Policy (2025/26).
[11] Lawcover (and Law Society of Tasmania), Cyber Risk Policy (v1.0) (2024).

(b) The ARNECC approach risks distorting the insurance market for law firms engaged in property and commercial law. There is a finite number of insurance companies willing to provide such coverage. Taking such a specific approach in the MPRs might lead to insurance companies being less open to negotiation on insurance coverage and premiums.

(c) $50,000 is likely to be only a starting point. While the level in the Draft MPRs might be available this year, global uncertainty can significantly and quickly affect reinsurance markets. Next year, a law firm might genuinely be unable to obtain the insurance coverage ARNECC has specified, through no fault of its own. If this occurs, the law firm will be in breach of the MPRs and liable to suspension of its registration—this outcome means the requirement should be abandoned.

(d) Each State has its own professional indemnity insurance arrangements. Setting a national standard in the ARNECC MPRs at some point may be unachievable for one or more jurisdictions, because of these variations.

41. In the Law Council's view, the draft MPRs should be amended to provide flexibility for Subscribers who are unable to meet the requirements, having attempted to comply in good faith. We suggest some equivalent to the current draft of Insurance Rule 0.62 under which a Subscriber must generally maintain appropriate levels of insurance reasonably necessary to ensure they are appropriately and adequately covered for risks associated with operating as a Subscriber.

42. A Subscriber should have an option available under which it is not deemed to breach the MPRs provided it can demonstrate it has made genuine efforts to implement insurance arrangements appropriate for its size, nature and complexity, and which the Subscriber considers adequately protects its business and clients.

43. If the proposed requirement for cyber security insurance is to be retained, sufficient lead time will be necessary for insurers to offer suitable products before Subscribers are required to prepare and comply with this new requirement. We suggest this should be at least 12 months from the finalisation and publication of Version 8 of the MPRs. Similar lead times should also be provided for each of the changes to Identity Agent insurance in Rule 1, so that the relevant timeframes are aligned.

44. Additionally, if Insurance Rule 0.5 is retained, it could be modified in the following respects:

- by inserting the words "other than for loss of funds" after "third party claims" in Rule 0.5(b);
- by including a definition of "cyber incidents" which is consistent with the definitions in commercially available cyber security policies; and
- by inserting the words "(subject to any reasonable waiting period)" after "business interruption" in Rule 0.5(c).

Schedule 8—Verification of Identity Standard

45. The Law Council would welcome further discussion with ARNECC about the scope of Verification of Identity (**VOI**) obligations, in particular in the context of the recent commencement of anti-money laundering and counter-terrorism financing (**AML/CTF**) obligations for relevant law firms in Australia.

46. The Verification of Identity Standard (**VOI Standard**), under Schedule 8 to the MPRs, was first developed in 2012 and adopted in participating jurisdictions in 2013. With the passing of time, advances in technology and improvements in best practice for the protection of personal information and documentation, we submit that consideration be given to revising the VOI Standard in two important respects.

47. First, Rule 2.1 of the VOI Standard requires the verification of identity to be conducted during a face-to-face in-person interview. With greater use of audio-visual means for client meetings, particularly in regional and remote areas, we suggest that this requirement is unduly restrictive and reduces the potential use of the VOI Standard. We request that Rule 2.1 of the VOI Standard expressly permit the verification of identity interview to be conducted using suitable audio-visual technology.

48. Second, Rule 3.3(b) of the VOI Standard requires the Identity Verifier to "retain copies of all Documents produced by the Person Being Identified and any Identity Declarant". This is an increasingly problematic aspect of the VOI Standard. In the experience of members of the legal profession, clients are often reluctant to permit their solicitor to retain copies of their identity documentation. An alternative practical approach increasingly adopted is to make a file note of the identification documents presented and verified, rather than take copies of the identification documents. Where law firms have access to the Commonwealth's Document Verification Service,[12] the need to make or retain copies of a client's identification documents would be removed.

49. The critical issue is the sighting of the identification documents, and verification that the documents are those of the client. Rule 2.2 of the VOI Standard requires the Identity Verifier to be satisfied that the person verified bears a reasonable likeness to the person depicted in a photographic identity document. In that context, a copy of the identity document serves as evidence that the Identity Verifier complied with Rule 2.2, but with attendant security risks, including a potential increase in the risk of being targeted by threat actors.

50. We suggest that ARNECC instead allow alternative forms of evidence an Identity Verifier could use to demonstrate compliance with the VOI Standard, and consider closely whether retaining copies of identity documents is reasonably necessary from a privacy perspective. We further note that the reduction of the retention of identification documents may also assist with the Subscriber meeting the standard required under a Cyber Security Framework.

---

[12] Australian Government, ID Match, About our services (Web Page).

51. The appropriateness of retaining copies of identity documents has recently been considered in the context of the expansion from 1 July 2026 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**) to include Tranche 2 entities, such as solicitors providing designated services.

52. Following 1 July 2026, small- and medium-sized firms subject to the AML/CTF framework must now comply with relevant provisions of the *Privacy Act 1988* (Cth). Law firms with a turnover of more than $3 million were already subject to these obligations.

53. The Office of the Australian Information Commissioner (**OAIC**) has released privacy guidance for reporting entities under the AML/CTF Act, which suggests the following in relation to retention of identification documents:

> *You must only retain the minimum information that you need. For example, if you need to keep records to demonstrate compliance with customer due diligence, you should only record personal information from identification documents relevant to your record keeping requirements (for example names, date of birth, residential address, date of expiry, passport/license number), the type of document, what you did to identify a customer, the outcome of your verification and analysis, identification or assessment of ML/TF risk.*
>
> *You should take reasonable steps in the circumstances to destroy (or de-identify) copies of full identification documents (such as driver's licenses or passports) after you no longer need them for your AML/CTF obligations or for another purpose under the Privacy Act or the APPs.*[13]

54. The OAIC Guidance suggests that firms should not keep copies of identity documents, unless there is a professional obligation to do so. While the ARNECC VOI standard might be a professional obligation justifying the keeping of copies, it would be timely to reconsider this position in the MPRs. Every time copies of identity documents are obtained, transferred and retained by entities, there is an increased risk of those documents being exposed to a data breach or unintentional release.

55. In light of recommended best practice, we submit that consideration be given to amending Rule 3.3.(b) of the VOI Standard to remove the requirement to retain copies of all Documents. If appropriate, this could be replaced with an obligation to record appropriate information in relation to all Documents produced by the Person Being Identified and any Identity Declarant.

56. Alternatively, a more appropriate obligation may be to require the Subscriber to enter into an arrangement with the Identity Agent under which the Subscriber can require the Identity Agent to deliver copies to the Subscriber, if needed, and that relevant information (such as licence number) can be extracted rather than a full copy made.

---

[13] Office of the Australian Information Commissioner, Privacy guidance for reporting entities under the AML/CTF Act (April 2026) 18.

Contact

57. If you have any queries regarding the contents of this letter, please do not hesitate to contact John Farrell, Executive Policy Lawyer [redacted]

Yours sincerely



Tania Wolff
President