

Our ref: PLC/PDL:RMgl100726

10 July 2026

Dr James Popple
Chief Executive Officer
Law Council of Australia
PO Box 5350
BRADDON ACT 2612

By e-mail: [REDACTED]

Dear Dr Popple,

**MODEL OPERATING REQUIREMENTS AND MODEL PARTICIPATION RULES - VERSION 8
CONSULTATION DRAFTS**

Thank you for the opportunity to contribute to the Law Council's submission to the Australian Registrars' National Electronic Conveyancing Council (**ARNECC**) in response to Model Operating Requirements Consultation Draft version 8 and Model Participation Rules Consultation Draft version 8 (**draft MPRs**). The Law Society's Property Law and Privacy and Data Law Committees contributed to this submission.

Draft MPRs

Rule 2.1 Definitions

We comment in relation to the following definitions which are introduced or amended in the draft MPRs.

Cyber Security Framework

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- (d) if any of the above is superseded, the cyber security framework that has superseded it, or such other alternative cyber security framework as is substantially equivalent to that Cyber Security Framework.

We support the flexibility inherent in the definition provided, as the three standards chosen 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 some large law firms have achieved certification under ISO Standard 27001, the costs of compliance with this standard are likely to be out of reach for smaller practices. It is therefore important to retain flexibility in providing a choice of standards available to achieve the proposed 'safe harbour' provided for under proposed Rule 7.11(b)(i), should a Subscriber choose to adopt that approach. We also suggest that further

precision is required regarding the elements of a particular standard to be met in order for a Subscriber to discharge their obligations under proposed Rule 7.11. 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), it is unclear with what level of that standard they would be required to comply.

We note that the Essential Eight (**E8**) framework could serve as a useful 'baseline' standard, of those specified. 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 assessments from reputable E8 assessors in order to ensure and demonstrate their compliance with it, 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 costs of assessments and remedial action to address any non-compliance.

Consideration could also be given to including the Information Security Manual (ISM),¹ developed by the ASD, as another framework captured in the definition of "Cyber Security Framework". The ISM which incorporates the E8 as a baseline and is a more detailed standard; it 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

Jeopardised Conveyancing Transaction

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.

In our view, this definition is unduly broad and open to subjective interpretation. In our view, the inclusion of Conveyancing Transactions which "could put at risk" the integrity of the Titles Register should be removed from the proposed revised definition.

Personal Information

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.

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

With the expanded role this definition will play with the proposed changes, we submit that the definition of Subscriber Systems must be limited to only those systems that are used in connection with a Conveyancing Transaction. This definition is not amended in the draft MPRs, but in our view it should be, given the wider role this definition now plays.

¹ Australian Government, Australian Signals Directorate, Information security manual <<https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism>>.

² For example, see the commentary on Information security and cyber security published by the Australian Government, Department of Finance <<https://sellingtogov.finance.gov.au/faq/security-requirements>>.

³ Australian Government, Australian Signals Directorate, Infosec Registered Assessors Program (IRAP) <<https://www.cyber.gov.au/business-government/protecting-devices-systems/assessment-evaluation-programs/irap>>.

The current definition of Subscriber Systems is:

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

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. It would be highly inappropriate for the Model Participation Rules (**MPRs**) to have general application to all systems of a law firm Subscriber, which may be an unintended consequence of the original broad drafting. Given the application of this definition in new proposed Rules, such as proposed Rule 7.11(a)(ii), we submit that the definition of “Subscriber Systems” must be expressly limited to those systems used in connection with a Conveyancing Transaction.

Rule 6.3 Client Authorisation

It is proposed to amend Rule 6.3 to remove the exemption for the provision of a Client Authorisation for caveats, priority notices, extensions of priority notices and withdrawals of priority notices. As to the proposed amendment to Rule 6.3, the Explanatory Notes provided by ARNECC⁴ cite “Technological advances mean that obtaining an urgent Client Authorisation for a Caveat or Priority Notice is now possible”. We are comfortable with the exemption being removed in relation to priority notices and their extension or withdrawal, but we oppose the exemption being removed for caveats. By their very nature caveats are time sensitive. In our view 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. We also note that 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. We submit 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

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.

In our view, the breadth of Rule 7.1(d) is unworkable, particularly where the Subscriber is a law firm, which would appear to mean implementation of MFA across the firm in areas that have no connection to the conduct of 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, in practical terms, would require the use of MFA for remote access by all of the law firm’s staff. In a larger firm, the majority of the law firm’s staff would have no involvement 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 account⁵ to an 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 are unable to support proposed Rule 7.1(d).

⁴ ARNECC, Model Participation Rules (MPR) Consultation Draft 8.01 – Explanatory Notes May 2026
<<https://www.arnecc.gov.au/wp-content/uploads/2026/05/Model-Participation-Rules-Version-8-Explanatory-Notes.pdf>>.

⁵ Proposed Rule 7(d)(iii) seeks to introduce MFA for all use of email accounts for all Users.

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 Electronic Lodgment Network (**ELN**). 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.⁶ Similarly, under clause 4.3.7 of the Sympli Subscriber Security Policy, access to the Sympli ELN requires the use of MFA.⁷ In our view, this is an appropriately targeted use of MFA in the eConveyancing system and no further requirements for MFA should be introduced. Consideration could instead be given to amending the Model Operating Requirements to mandate that Electronic Lodgement Network Operators must require Subscribers use MFA to access the ELN to embed the current practice as a regulatory requirement. In our view, this would be an appropriate and targeted use of MFA in maintaining the security of the eConveyancing system overall.

We note that there are varying degrees of adoption of MFA in law firms already, but the implementation costs and compliance burden of stipulating MFA as proposed may, as stated, be too onerous, particularly 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. While we acknowledge the benefits of MFA, and support law firms choosing to adopt MFA, it is not appropriate, in our view, for ARNECC to mandate the specific use of MFA as proposed, and we submit that Rule 7.1(d) should be deleted. If proposed Rule 7.1 is adopted, we suggest a clear commencement date for Rule 7.1 should be inserted, and this date should be at least 12 months from the finalisation and publication of MPR version 8.

Rule 7.11 Secure use of systems

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 note the flexibility provided, which is important due to the varied size, nature, location and resources of law firms.

As there will also be variation amongst law firms as to their current cyber security posture, we suggest it would be appropriate to provide a lead time to enable education and preparation time, including implementing the necessary system controls and obtaining certification where that is the approach chosen by the Subscriber. We suggest this should be at least 12 months from the finalisation and publication of MPR version 8. 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.

In relation to proposed Rule 7.11(a)(iv), in addition to deleting the redundant words “use of”, we suggest the reference to email accounts should be confined to the Subscriber’s email accounts used in connection with the conduct of a Conveyancing Transaction.

Should the proposed changes proceed, we anticipate that Model Participation Rules Guidance Note 8 “System Security & Integrity”⁸ will be updated. We suggest that in connection with proposed Rule 7.11, the Guidance Note should be expanded to include:

- Examples of what factors might be considered in relation to the obligation to take reasonable steps under proposed Rule 7.11(a).

⁶ PEXA Subscriber Security Policy Version 4, 5 August 2025, effective from October 9th 2025 <<https://www.pexa.com.au/subscriber-security-policy/>>.

⁷ Sympli Subscriber Security Policy Version 6, May 2025 <<https://www.sympli.com.au/wp-content/uploads/Subscriber-Security-Policy-May-2025-website-version.pdf>>.

⁸ ARNECC, MPR Guidance Note 8 – System Security & Integrity <<https://www.arnecc.gov.au/wp-content/uploads/2024/08/MPR-Guidance-Note-8-System-Security-Integrity-Updated.pdf>>.

- Introductory information about the cyber security standards which 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 Standard 27001 audits are undertaken by accredited third party assessors who issue a certificate.

We also note that Model Participation Rules Guidance Note 6 “Compliance Examinations”⁹ will likely need to be updated.

Schedule 6 Insurance Rules

We note that Insurance Rule 0.3(f) (which we understand should read 1.3(f)), requires coverage to be extended to “criminal or malicious act or omission by the Subscriber or the Subscriber’s principals, Officers or employees in connection with Conveyancing Transactions”. 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 who would generally be relying on the deeming provision in Insurance Rule 3.1(a) (which should read 4.1(a)) but will be relevant for other Subscribers.

We have serious concerns with Insurance Rule 0.5 (which we understand should read 1.5), and the requirements set out 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. We are concerned that 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. Our further concerns with Insurance Rule 0.5 are set out in the following paragraphs.

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 fraud. 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.

⁹ ARNECC, MPR Guidance Note 6 – Compliance Examinations <<https://www.arnecc.gov.au/wp-content/uploads/2024/08/MP2FF41.pdf>>.

¹⁰ A copy of the terms of the current Lawcover professional indemnity insurance policy is available at <<https://www.lawcover.com.au/wp-content/uploads/2025/03/202526-PII-Policy-Wording-SAMPLE.pdf>>.

¹¹ A copy of the terms of the current Lawcover cyber risk policy is available at <<https://www.lawcover.com.au/wp-content/uploads/2024/05/Lawcover-Cyber-Risk-Policy.pdf>>.

However, notwithstanding that Lawcover's cyber risk policy potentially already provides a limited degree of coverage, we do not support cyber security insurance for enterprise risks (including incident response, business interruption and data/system recovery) being a requirement in the MPRs. Similarly to the concerns already flagged above, such a requirement may be problematic if insurers such as Lawcover adjust or discontinue this policy in the future. First party business risks and insurance are a much broader issue for legal practices and other Subscribers and 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, and for these reasons we are unable to support the inclusion of Insurance Rule 0.5 as drafted.

If the requirement for cyber security insurance proceeds, we suggest that sufficient lead time will be necessary for Subscribers to prepare and comply with this new requirement. We suggest this should be at least 12 months from the finalisation and publication of MPR version 8. Similar lead times should also be provided for each of the changes to Identity Agent insurance in Rule 1 (which we understand should read Rule 2), as the relevant time frames should be aligned in our view. We also submit that, if retained, Insurance Rule 0.5 should 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).

We understand that Lawcover will be making its own submissions which are likely to be more detailed in relation to insurance issues arising out of the proposed rules. In the interests of transparency, we note that Lawcover is a wholly owned subsidiary of the Law Society of New South Wales, that operates under a separate and independent board and management team.

Schedule 8 Verification of Identity Standard

The Verification of Identity Standard (**VOI Standard**), under the Model Participation Rules, was first developed in 2012, and adopted in participating jurisdictions in 2013. With the effluxion 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.

Firstly, 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 submit that consideration be given to amending Rule 2.1 of the VOI Standard to expressly permit the verification of identity interview to be conducted using audio-visual technology.

Secondly, 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 our members' experience, in light of the prevalence of data breaches, clients are, understandably, 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.

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. 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.

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. The Office of the Australian Information Commissioner has released “Privacy guidance for reporting entities under the AML/CTF Act”¹² 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

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.

Thank you for the opportunity to comment. Any questions in relation to this letter should be directed to Gabrielle Lea, Senior Policy Lawyer, at gabrielle.lea@lawsociety.com.au or on (02) 9926 0375.

Yours sincerely,



Ronan MacSweeney
President

¹² Office of the Australian Information Commissioner “Privacy guidance for reporting entities under the AML/CTF Act” April 2026, <https://www.oaic.gov.au/__data/assets/pdf_file/0021/263046/OAIC-Guide-to-privacy-for-reporting-entities-under-the-AML-CTF-Act-updated-April-2026.pdf>.

¹³ Ibid 18.