ARNECC

AUSTRALIAN REGISTRARS NATIONAL ELECTRONIC CONVEYANCING COUNCIL

Security-related obligations under the electronic conveyancing regulatory framework

Discussion Paper

October 2024

Contents

Overview

Upholding the security and integrity of the land title Registers in each State and Territory, Electronic Lodgment Networks (ELNs), and of the wider conveyancing ecosystem is critical.

Accordingly, and noting the security landscape is changing Australia-wide and worldwide, the Australian Registrars' National Electronic Conveyancing Council (ARNECC) is seeking feedback on various security and evidence retention related obligations under the:

- Model Operating Requirements (MOR), approved by ARNECC and determined by Registrars under section 22 of the *Electronic Conveyancing National Law* (ECNL) as jurisdictional Operating Requirements (OR), that apply to Electronic Lodgment Network Operators (ELNOs); and

- Model Participation Rules (MPR), approved by ARNECC and determined by Registrars under section 23 of the ECNL as jurisdictional Participation Rules (PR), that apply to Subscribers to ELNs, being predominantly conveyancers, lawyers, and financial institutions.

Due to the potential impact of the possible approaches outlined in this discussion paper to ELNOs and Subscribers, ARNECC wishes to consult on this paper before publishing related consultation drafts of the MOR and MPR after Version 7. ARNECC welcomes feedback on relevant matters regarding the MORs and MPRs additional to those raised in this paper.

Feedback may be submitted to chair@arnecc.gov.au by 5:00pm (Australian Eastern Standard Time) on Friday, 6 December 2024.

Note:

- *Terms capitalised in this paper have the meaning given to them in the current MOR and MPR*
- *This paper largely focusses on security related obligations under the MPR. ARNECC is also undertaking a thorough review of security-related obligations under the MOR.*

Existing security-related obligations

There are several obligations regarding system security and integrity with which ELNOs and Subscribers must comply. These existing obligations aim to provide a comprehensive framework to secure the systems used in electronic conveyancing and proactively manage the risk of fraud and misuse. Additionally, some security measures are in place to facilitate the efficient operations of systems.

Some key obligations include:

- **Maintaining system security and integrity** – the ELNO must keep current a documented Information Security Management System in relation to its operations (MOR 7.1).

- A Subscriber must take reasonable steps to comply with the security policy of each ELNO (MPR 7.1).

- **Limiting access to authorised persons only** – Subscribers must take reasonable steps to verify the identity of each of its Signers before initial allocation of a Digital Certificate, Subscriber Administrators prior to their appointment, and Users prior to being given access to an ELN (MPR 6.5.1). Subscribers must also ensure that Users meet the fit and proper requirements before accessing an ELN (MPR 7.2).

- Prior to the initial allocation of a Digital Certificate to a Signer or prior to the appointment of a Subscriber Administrator, a police background check must be conducted on the Signer and Subscriber Administrator (MPR 7.2). If a Subscriber no longer intends a person to be a User of an ELN, a Subscriber can revoke the User's access and use of the ELN (MPR 7.8).

- **Keeping Digital Certificates safe and secure** – the ELNO must ensure that Digital Certificates used in the ELN accord with the Gatekeeper PKI framework (MOR 7.6.2). Subscribers must also take reasonable steps to ensure that:
    - a Digital Certificate is only used to Digitally Sign by the Signer to whom it is allocated; and
    - Signers do not allow any other Person to use their Access Credentials and Digital Certificates; and
    - Signers keep the Digital Certificate allocated to them safe and secure in the Signer's control; and
    - Access Credentials are only used to access an ELN by the User to whom the Access Credentials belong; and
    - Other Users do not allow any other Person to use their Access Credentials (MPR 7.5.5).

- **Protecting Land Information** – the ELNO must ensure that any computer infrastructure that stores or processes Land Information (as defined in the MOR) is located within Australia (MOR 7.5).

- **Undertaking annual system testing** – the ELNO must engage an appropriately qualified independent security professional to undertake a vulnerability assessment and penetration test of its ELNO System and promptly implement any Essential Recommendations arising from the testing (MOR 7.13).

- **Notifying relevant parties of any compromised transactions** – the ELNO must immediately notify the Registrar and any other affected parties such as Subscriber(s) or another ELNO if there is a Jeopardised Conveyancing Transaction or Compromised Security Item (MOR 7.9 and 7.10). This requirement also applies to Subscribers under MPR 7.7 and 7.9 who must notify the ELNO, Registrar and other Participating Subscribers.

A failure to comply with any of the above obligations may lead to a restriction, suspension or termination of the Subscriber's access to and use of an ELN or a suspension or revocation of the ELNO's approval to operate an ELN (i.e. MPR 9 and MOR 20.1).

There are other obligations such as verification of identity, establishing a person's right to deal, under the MPR and retention of supporting evidence that seek to uphold the security and integrity of the land title Registers.

These obligations, and various other security-related matters, are discussed below.

1. Security policies for Subscribers and monitoring compliance

1.1 Context

Under the MOR, an ELNO must establish, implement, operate, monitor, review maintain and keep current a documented Information Security Management System (ISMS) that includes a comprehensive Subscriber security policy with which Subscribers and Users of an ELN must comply (MOR 7.1).

Subscribers must take reasonable steps to comply with the Subscriber security policy of an ELNO with which they have a current Participation Agreement (MPR 7.1 and 7.2). Under that security policy, Subscriber obligations (required security controls or measures) include:

- installing specified virus protection software on their computers;
- protection of security items such as User Access Credentials, Passphrases, Digital Certificates and related Private Keys; and
- training and monitoring Users in cyber security awareness (MOR 7.1).

1.2 Matters for consideration

As a part of its ISMS, an ELNO is required to maintain a documented Subscriber review process, to review the compliance of Subscribers with the Participation Rules (bar some exceptions – MOR 14.7). However, there is no specific requirement for ELNOs to assess the compliance of Subscribers with the ELNO's Subscriber security policy. Also, there is no requirement for Subscribers to comply with, or have the above security controls and measures audited against an established cyber security framework.

While this current approach under the MOR and MPR provides Subscribers flexibility, it does not set standardised minimum cyber security controls that Subscribers must implement. This means that Subscribers could be using varying qualities of cyber security controls. Subscribers with less security maturity could compromise the security of the relevant ELN and the security of other Subscribers connected to that ELN.

It has been separately suggested to ARNECC that ELNO Subscriber security policies vary and there is limited assurance that the security controls defined in an ELNO's Subscriber security policy are appropriate to address the threats facing Subscribers.

ARNECC is considering ways to ensure that both ELNOs and Subscribers maintain appropriate cyber security controls, to prevent poor security practices that could compromise the security of ELNs and land registries.

1.3 Possible approaches

MOR 7.1 could be amended to require ELNOs to perform sampled assessments of Subscribers' compliance with the ELNO's Subscriber security policy, using a reasonable representative sample of Subscribers within each operating jurisdiction.

Further or alternatively, the MPR could stipulate that all Subscribers are required, at a minimum, to comply with an established cyber security framework or a set of identified and agreed standards. ARNECC seeks feedback from industry on possible frameworks or standards.

Standard in this regard means:

a. a current standard, (or in the absence of a standard, a handbook) published by Standards Australia Ltd, its successor or any national body having a similar function; or
b. where there is no current relevant standard published by Standards Australia Ltd, a current standard published by the International Organisation for Standardisation.

ARNECC is aware of the Essential Eight cyber security framework – which is a mitigation strategy designed by the Australian Signals Directorate, Australian Cyber Security Centre primarily to protect organisations' internet-connected networks.

ARNECC is also aware that there are different levels under that framework. For example, Maturity Level One (of Three Levels) focuses on malicious actors that opportunistically seek common weaknesses in targets, rather than investing heavily in gaining access to a specific target (https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model). ARNECC seeks industry feedback on the appropriate framework and level.

Request for feedback

For the above section 1 of the paper, please:

1. provide your comments on the matters for consideration and possible approaches, for the MOR and/or MPR; and
2. detail any other possible approaches that you would like ARNECC to consider, with reasons.

Note: when providing comments with reasons, please consider the following prompts and provide examples if possible:

a) is this an issue that has affected you and/or your stakeholders?

b) how would the possible approaches affect you and/or your stakeholders?

2. Multi-Factor Authentication

2.1 Context

There are various security risks that come with remotely accessing computer applications and systems, such as exposure to information technology security vulnerabilities, unauthorised access, and potential data breaches.

Multi-factor authentication (MFA) is understood to be a foundational cyber security control that greatly reduces the risk of account compromise, including business email compromise (BEC). BEC in relation to high-value property settlements is occurring at a high enough frequency to be specifically featured in the Australian Cyber Security Centre's 2022-2023 Cyber Threat Report.

Investigations into BEC suggest property settlements are being targeted. This is likely due to the high volume and value of transactions as well as increases in property values.

2.2 Matters for consideration

While MFA is required to log into an ELN, there is currently no requirement for Subscribers to implement MFA to access applications they use that could relate to an electronic conveyancing transaction, for example, emails, cloud storage, file management software and practice management systems.

2.3 Possible approaches

The MPR could be amended to include a requirement that Subscribers must implement MFA for all remote access (including Virtual Private Networks), administrative accounts and email accounts used to access an ELN.

An alternative could be to amend the MOR to stipulate that ELNOs' Subscriber security policy must include a requirement that Subscribers implement MFA for all remote access.

ARNECC acknowledges that many Subscribers may have already implemented and are using MFA in line with the sensitive nature of the work and information stored in emails. Subscribers who have already adopted MFA should not have difficulty adhering to this requirement, but Subscribers yet to adopt MFA may need time to implement it.

ARNECC is aware that MFA is only one of a wide range of security protection measures that should be employed by all ELNOs and Subscribers. Additional measures include but are not limited to strong passwords and maintaining and regularly updating systems and applications used.

ARNECC seeks feedback on expanding the requirement for MFA beyond logging into an ELN. Further to the above, ARNECC seeks feedback as to whether any other additional security measures should be considered for inclusion in the MOR and/or MPR.

Request for feedback

For the above section 2 of the paper, please:

1. provide your comments on the matters for consideration and possible approaches, for the MOR and/or MPR; and
2. detail any other possible approaches that you would like ARNECC to consider, with reasons.

Note: when providing comments with reasons, please consider the following prompts and provide examples if possible:

a) is this an issue that has affected you and/or your stakeholders?

b) how would the possible approaches affect you and/or your stakeholders?

3. Verification of Identity Standard and reasonable steps

3.1 Context

Verification of Identity (VOI) is a critical due diligence obligation in the electronic conveyancing process, establishing 'checks and balances' to minimise risks such as identity theft and fraud associated with conveyancing transactions.

Under the MPR, Identity Verifiers (ordinarily a Subscriber or their appointed Identity Agent) must take reasonable steps to verify the identity of:

- Clients, or each of their Client Agents
- Mortgagors
- Signers, before being given their Digital Certificate used to digitally sign Registry Instruments and other electronic Documents, lodgment instructions etc in the Electronic Workspace
- Subscriber Administrators, before being appointed as a Subscriber Administrator
- Users, before being given access to an ELN,

by either:

a. applying the VOI Standard as set out in Schedule 8 of the MPR (see MPR rule 6.5.1) or
b. verifying the identity in some other way that constitutes the taking of reasonable steps (MPR rule 6.5.2).

Identity verifiers who apply the VOI Standard are deemed to have taken reasonable steps provided the Subscriber was not required to take further steps under MPR 6.5.3 (MPR rule 6.5.6).

<u>The VOI Standard</u>

The VOI Standard in the MPR adopts a face-to-face regime, coupled with the production of original identification documents to ensure that the person being identified is of reasonable likeness (MPR Schedule 8).

The VOI Standard is based on the *Gold Standard Enrolment Framework*, developed by the Council of Australian Governments under the National Identity Security Strategy and adopted as the recommended whole of government framework for establishing proof of identity. It proposed four separate categories of proof of identity documentation which included:

a. evidence of commencement of identity in Australia
b. a linkage between identity and the person (photo and signature)
c. evidence of an identity operating in the community
d. evidence of residential address (only if not provided by Category B or C).

On the advice of independent experts, ARNECC adopted this model under the MOR and MPR and modified it to better suit the needs of Identity Verifiers.

When the VOI Standard has been complied with, Subscribers have the benefit of being deemed to have taken reasonable steps. This is particularly relevant when Subscribers are required to prove reasonable steps in compliance with legislation.
For example, some jurisdictions have a statutory obligation for a mortgagee to take reasonable steps to verify the identity of a mortgagor.

Reasonable steps

The reasonable steps VOI option (MPR rule 6.5.2) was included in the MPR to provide flexibility to Subscribers.

Circumstances for verifying a person's identity can vary significantly. Subscribers may be unable to meet their clients in person to complete VOI in accordance with the VOI Standard and an Identity Agent may not be available. In these circumstances, Subscribers may determine that a departure from the VOI Standard would be reasonable. ARNECC has published guidance notes on VOI, including the concept of reasonable steps (MPR Guidance Note 2: Verification of Identity).

Digital VOI options

ARNECC acknowledges that the VOI environment is changing – digital VOI options are developing, and a federal legislative framework is being introduced to create an economy-wide Digital ID system in Australia (Digital ID Build, 2024). ARNECC is monitoring the progression of that legislative framework and the Commonwealth Government's approach to digital VOI. Closer to implementation, ARNECC will consider the new framework. However, until there are legislative digital VOI standards, there is no authoritative basis for allowing digital platforms to be used as part of the MPR VOI Standard.

In the meantime, Subscribers may make their own assessment as to whether digital VOI constitutes the taking of reasonable steps for VOI of the relevant person in the circumstances.

3.2 Matters for consideration

ARNECC has previously consulted on the reasonable steps VOI option and wishes to raise it again to ensure that the VOI regime under the MPR remains effective, in terms of upholding the security of conveyancing transactions.

3.3 Possible approaches

VOI Standard in all instances
Subscribers could be required to apply the VOI Standard in all instances (remove the option to take other reasonable steps)

Applying the VOI Standard in all cases mitigates the risk caused by the ambiguity of a reasonable steps option, under which varying approaches can be taken. Further, in recent years an evolving cybercrime landscape has required greater scrutiny of the safeguards in place to mitigate the risk of identity crime. Accordingly, removing the reasonable steps VOI option from the MPR could be desirable from a risk perspective.

ARNECC acknowledges though that removing the reasonable steps VOI option would place a constraint on Subscribers and could have negative ramifications for different stakeholders. That is, there would be no flexibility to carry out VOI other than through a face-to-face meeting. This may cause issues for:

- Clients based in rural or remote communities
- Clients based overseas – where clients would need to make a trip and potentially incur extra costs to complete VOI at an Australian embassy, high commission or consulate
- Subscribers who rely on the reasonable steps option to use digital VOI as part of their practice.

However, the MPR does allow Subscribers to engage the services of an Identity Agent to carry out VOI in accordance with the VOI Standard, which offers some flexibility in carrying out VOI.

VOI Standard in certain conveyancing transactions
Alternatively, Subscribers could be required to apply the VOI Standard for certain conveyancing transaction types only (retaining the option in other instances to take reasonable steps).

This approach adopts a risk-based approach to VOI obligations whereby Subscribers must apply the VOI Standard when dealing with certain conveyancing transaction types considered to be of increased risk, however, for all other conveyancing transaction types, retain the discretion to apply the VOI Standard or take reasonable steps to undertake VOI.

Increased risk might be relevant for:

- high-value conveyancing transactions
- mortgages and transfers involving a high monetary consideration
- mortgages and transfers between related parties
- an application to change a name or address in the land title Registers (the name of this dealing type varies between jurisdictions) - for a change of name, the only matter underpinning the dealing is verification of the applicant's identity
- a VOI where the circumstances set out in MPR 6.5.3 apply.

The aim of this approach is to reduce the risk profile for particular conveyancing transactions, while retaining a level of flexibility for Subscribers to meet their obligations.

Request for feedback

For the above section 3 of the paper, please:

1. provide your comments on the matters for consideration and possible approaches, for the MOR and/or MPR; and
2. detail any other possible approaches that you would like ARNECC to consider, with reasons.

Note: when providing comments with reasons, please consider the following prompts and provide examples if possible:

a) is this an issue that has affected you and/or your stakeholders?

b) how would the possible approaches affect you and/or your stakeholders?

4. Supporting evidence obligations in the MPR

4.1 Context

Currently, a Subscriber must retain the evidence supporting an electronic Registry Instrument or other electronic Document for at least seven years from the date of lodgment of the electronic Registry Instrument, or other electronic Document. Evidence required to be retained includes:

- any evidence required by a Duty Authority
- any Client Authorisation and any evidence supporting that Client Authorisation
- any evidence supporting a party's right to enter into the conveyancing transaction
- any evidence supporting VOI (MPR rule 6.6).

Evidence is required to be retained to demonstrate that the conveyancing transaction was completed in accordance with legislative and other requirements, and that the certifications (under the Certification Rules in Schedule 3 of the MPR) were validly given.

Evidence may be required to be produced as part of a Compliance Examination (under Schedule 5 of the MPR) to ascertain whether a Subscriber has complied with the MPR, or for investigating any suspected or alleged case of misconduct.

If a dispute arises in relation to a conveyancing transaction, it is also of benefit to a Subscriber to be able to demonstrate in court proceedings that the transaction was completed in accordance with legislative and other requirements.

When the supporting evidence MPR 6.6 was included in the MPR in 2013, storage of information for a period of seven years was understood to be a standard industry requirement.

4.2 Matters for consideration

The secure storage of data for an appropriate length of time especially data containing Personal Information is becoming increasingly important, considering the expanding digital environment and growing threat of cybercrime.

ARNECC seeks feedback on supporting evidence MPR 6.6, including the current seven-year retention period.

In particular, ARNECC would like to understand any alternatives that could be used in relation to Personal Information. If alternatives, are proposed which mean that paragraph 3.3(b) of the VOI Standard requiring retention of copies of identity Documents cannot be complied with, Subscribers would need to evidence and if necessary, prove to a Court how they took reasonable steps rather than being deemed to have taken reasonable steps.

Request for feedback

For the above section 4 of the paper, please:

1. provide your comments on the matters for consideration and possible approaches, for the MOR and/or MPR; and
2. detail any other possible approaches that you would like ARNECC to consider, with reasons.

Note: when providing comments with reasons, please consider the following prompts and provide examples if possible:

a) is this an issue that has affected you and/or your stakeholders?

b) how would the possible approaches affect you and/or your stakeholders?