NOTICE TO SUBSCRIBERS

Number	2019-NS1
Subject	**Cyber Security**
Purpose	To raise Subscriber awareness of their obligations regarding system security and integrity and provide advance notification of proposed amendments to the MOR and MPR version 6.

In an increasingly digital world, the need for effective cyber security is vital. In particular where our nation's conveyancing industry systems are being used daily to transact deals worth multi-millions of dollars, which by its nature may attract hackers and cyber criminals who seek to exploit these systems and access funds illegally.

The systems used by the electronic conveyancing industry must be trusted. System operators must apply industry best practices which mitigate fraud and misuse by unauthorised parties.

In this environment, ARNECC engaged Kinetic IT to provide an independent assessment of the cyber security requirements currently placed on Electronic Lodgment Network Operators (ELNOs) and Subscribers under the Model Operating Requirements (MOR) and the Model Participation Rules (MPR), to understand whether they represent industry best practice for mitigating against cyber fraud within the boundaries of what is within the Registrar's power under the Electronic Conveyancing National Law to require.

The challenge presented to Kinetic IT was to perform an accurate and comprehensive threat and risk assessment of the emerging technology platforms used to facilitate electronic conveyancing across Australia, and then review these in the context of today's threat landscape.

Kinetic IT's report to ARNECC earlier this year highlighted the importance of trust in the use of electronic conveyancing services as the industry continues its digital transformation journey. The security evaluation outcomes support the principle that the trust is well-placed.

The threats and risks identified by Kinetic IT support future enhancements to the MOR and MPR and are aligned to ARNECC's vision to continually improve the security posture of the electronic conveyancing industry, ELNOs and Subscribers. ARNECC has carefully considered the report recommendations and a number of those recommendations will be incorporated into Version 6 of the MOR and the MPR to strengthen provisions including, but not limited to:

- Use of Access Credentials and Digital Certificates
- Cyber security education and awareness of ELNO security policies

Another area of vulnerability highlighted in the report related to the risks surrounding the current Verification of Identity (VOI) provisions and what constitutes "reasonable steps" to identify clients. Reasonable steps can be interpreted very broadly and provides little or no assurance for the prevention of risks such as identity theft and fraud. As a result of these findings, amendments are proposed to be made to the VOI provisions in Version 6 of the MPR. A strong VOI standard helps in preventing the compromise of Subscriber systems as well as the potential escalation to the ELNO platform.

ARNECC will continue to implement security improvements to ensure cyber risks are proactively managed, including the ongoing reinforcement and communication of best practice cyber security awareness principles to ELNOs and Subscribers.

It is anticipated that the draft Version 6 MOR and MPR will be released for consultation in December 2019 and an industry forum will be arranged early in 2020 to provide the opportunity for Stakeholders to ask questions and discuss the changes.

Date of Issue	November 2019
Enquiries	The Land Registry in your State or Territory.

Notices to Subscribers are published at http://www.arnecc.gov.au/publications/notices_to_subscribers.