Submission No 1

INQUIRY INTO WHETHER VICTORIA SHOULD PARTICIPATE IN A NATIONAL ELECTORAL ROLL PLATFORM

Organisation: Electoral Council of Australia and New Zealand

Date Received: 21 October 2021

EMC Submission No. 1
Received 21 October 2021

Electoral Council of Australia & New Zealand

Submission to the Victorian Parliament's inquiry into whether Victoria should participate in a national electoral roll platform

Background

In July 2017 all Australian Electoral Commissioners wrote to Commonwealth, State and Territory First Ministers requesting that the issue of cyber security for Australia's election systems be placed on the COAG agenda.

A primary factor which led to the decision by ECANZ to approach First Ministers was an appreciation of the growing cyber security risks to, and vulnerabilities of, Australia's electoral infrastructure. With the increasing use of information technology in the delivery of electoral services there has been a related increase in the cyber threats faced by election management bodies (EMBs).

Australian Electoral Commissioners have agreed that there should be a coordinated national focus on the issue of electoral cyber security. The loss of public confidence in the integrity of one jurisdiction's electoral systems has the potential for a loss of confidence in all Australian electoral systems. A failure in electoral cyber security could also undermine both the willingness of electors to participate in election events and their acceptance of election results.

In a May 2017 report titled report – *Securing Democracy in the digital age* - the Australian Strategic Policy Institute (APSI) stated:

> *Public trust in the reliability and integrity of the electoral process is the foundation of the social contract between the governing and the governed in liberal democracies, so citizens must be able to trust that the computer systems responsible for handling the execution of an election will deliver an accurate result. (p.3)*

The issue of cyber-related election risks has been further examined by ASPI in an October 2020 report titled *Cyber-enabled foreign interference in elections and referendums*.

This matter was considered at COAG meetings in February and December 2018. At that latter meeting, COAG agreed to establish and support a Commonwealth-State working group of electoral commissions, electoral policy leads, the National Counter Foreign Interference Coordinator, and the National Cyber Security Adviser to strengthen the security of Australia's electoral systems, data and processes.

On 18 February 2019 the Prime Minister issued a public statement that:

> *Australia's democratic process is our greatest asset: our most critical piece of national infrastructure. Public confidence in the integrity of our democratic processes is an essential element of Australian sovereignty and governance.*

The security of Australia's electoral systems has also recently been considered by the Commonwealth Parliament's Joint Committee on Intelligence and Security in its *Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018*. At paragraph 3.74 of its September 2021 report the Committee observed:

> *Cyber-enabled operations spanning disinformation, data theft and technical disruption render democratic infrastructure vulnerable in new ways. Such operations, as witnessed in the 2020 presidential election in the United States, target political parties, news, and social media, and have the potential to affect broader public confidence in democratic systems.*

Pursuant to the COAG agreement, the Inter-Jurisdictional Working Group on Electoral Integrity and Security (IWGEIS) was formed, with its first meeting being held on 28 February 2019. Standing membership of IWGEIS is comprised of all Australian Electoral Commissioners, representatives from Commonwealth/State/Territory central and electoral policy agencies, the National Counter Foreign Interference Coordinator, and the Head of the Australian Cyber Security Centre.

IWGEIS deliberations

Each of Australia's nine Electoral Commissions runs its own election systems. The age and cyber security robustness of those systems varies from jurisdiction to jurisdiction, as does the capacity (financial and technical expertise) to maintain, upgrade and replace them. It is expected that cyber security threats to Australia's electoral systems will continue to increase. Individual Australian jurisdictions (and their EMBs) have limited capability and capacity to address these threats.

Through IWGEIS, all jurisdictions have agreed to explore options for a possible national platform to deliver electoral systems. The platform is envisaged as a secure information technology hosting environment which provides a shared services capability for EMBs. This platform could, in the long term, provide access to any number of electoral systems.

IWGEIS has established a working party to investigate possible IT systems, costings and governance arrangements for the platform. Electoral systems which have been identified for possible consideration for hosting on the platform include:

- electoral roll
- temporary workforce management
- device management
- data analytics and reporting
- venue management
- electronic mark-off
- learning management

Core features to be examined in designing the platform's operating model include such matters as:

- maintenance of compliance with Australian cyber security standards
- capacity to respond to multiple jurisdictional demands, including the running of concurrent electoral events
- scalability, with the ability to progressively incorporate additional electoral systems
- flexibility to enable individual EMBs to begin using individual services provided though the national platform over time, e.g. as their current systems reach end-of-life
- adaptive enough to accommodate legislative differences between jurisdictions (each jurisdiction would need to consider whether legislative changes would be required to facilitate their participation in this proposal)

The following threshold issues have been identified as requiring resolution in developing a possible platform.

Governance – An inter-jurisdictionally acceptable governance arrangement would need to be established to oversee the platform's operations and ongoing development. A fundamental requirement of any such arrangement is that the independence of EMBs, and their electoral operations and associated legislative responsibilities, is recognised and maintained.

Funding – Any possible platform would require funding, including the provision of upfront capital, for its establishment and operation. Having in mind the ongoing costs of maintaining, upgrading and replacing election systems in nine separate jurisdictions, operation of a platform should lead to financial and resource efficiencies. Having said this, the introduction of such a platform should not be viewed as a cost savings exercise. Developing the platform, and purchasing and maintaining the systems it would host, would require the commitment of significant resources by governments. Cost-sharing arrangements would be a matter for agreement by those governments.

Timing – This is not a 'big bang' proposal. Leaving aside the time required to establish a platform and its governance arrangements, it would not be feasible to migrate all relevant electoral systems into a platform in a single step. An iterative approach would be needed to gradually feed electoral systems into a possible platform. Depending on their replacement program for individual systems, each jurisdiction will have its own views (and needs) regarding usage of electoral systems hosted on such a platform.

The agreement of individual Federal, State and Territory governments would need to be obtained in order for jurisdictions to participate in a possible platform to host electoral systems. It should be noted that no proposal relating to the platform's creation has yet been submitted to Australian governments for their consideration.

IWGEIS examination of this proposal is ongoing.