Office of the Victorian Information Commissioner

t 1300 006 842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D21/17219

22 October 2021

Mr Lee Tarlamis OAM
Chair
Electoral Matters Committee
Parliament of Victoria

By email only: emc@parliament.vic.gov.au

Dear Mr Tarlamis,

Inquiry into whether Victoria should participate in a national electoral roll platform

Thank you for the opportunity to provide comment on the Electoral Matters Committee's inquiry into whether Victoria should participate in a national electoral roll platform.

The Office of the Victorian Information Commissioner (**OVIC**) has a unique regulatory focus, with combined oversight of information security, privacy, and freedom of information in Victoria, administering the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) and the *Freedom of Information Act 1982* (Vic).

Since 2014, OVIC has been responsible for setting the Victorian Protective Data Security Standards (**VPDSS**) and monitoring and assuring the security of public sector information against the Standards, under the Victorian Protective Data Security Framework (**VPDSF**).[1] Victoria is the only jurisdiction in Australia with legislated information security standards. These standards aim to ensure Victorian public sector (**VPS**) entities are appropriately protecting the confidentiality, integrity, and availability of public sector information and information systems against security risks.

Consequently, OVIC is familiar with the strategic issues raised by the terms of reference of this inquiry. This submission does not make a recommendation as to whether Victoria should or should not participate in a national electoral role platform. Rather, this submission details a range of matters that may impact on the future confidentiality, integrity and availability of Victoria's electoral roll information, including:

- The information security risks relevant to the future of Victoria's electoral roll—regardless of whether it is integrated with a future national electoral roll platform or the status quo is maintained; and
- A consideration of best practice regulatory strategies that would support and promote the security of Victoria's electoral roll information.

Information security risks

1. Best practice information security risk mitigation measures must be proportional to both the value of the information asset being protected, and the risk of the asset being compromised. The inherent value of protecting the confidentiality, integrity and availability of Victoria's electoral roll information is plain: the public's trust and confidence in Victoria's democracy is dependent on the ongoing security of

[1] Part 4 of the PDP Act provides authority for developing the VPDSF and setting the VPDSS.

electoral information systems. Less plain is the future risk associated with how this information could be compromised. Any future electoral roll system must consider the risks identified in previous incidents and seek to mitigate these.

Geopolitical risk

2. The Victorian Electoral Commission (**VEC**) and the Australian Electoral Commission (**AEC**) both operate in an increasingly insecure global security environment. This insecurity represents an inherent risk to critical infrastructure that facilitates essential government service delivery.

The impact of cyber incidents in comparative democratic jurisdictions

3. Autocratic nation-states revealed their hand during the two most recent United States presidential elections. By deploying offensive cyber capabilities to target the infrastructure that is responsible for securing the integrity of democratic elections, public trust in the liberal social contract can be eroded. Relevantly:

    - In the 2016 US presidential election, the Russian Federation targeted the election infrastructure of all fifty US states. Here, an autocratic nation-state advanced its geopolitical objectives by exploiting infrastructure vulnerabilities in US electoral systems. According to the US Senate Intelligence Committee, the "unprecedented level of activity against state election infrastructure" positioned Russia to delete or change election data in some states, which was mostly undetected by both state and federal officials at the time of the election.[2]

    - Russia and the Islamic Republic of Iran further attempted to interfere with the 2020 US presidential election. The US Intelligence Community reported that the cyberattacks aimed to undermine "public confidence in the electoral process" and to exacerbate "socio-political divisions".[3] As a result, the 2021 Capital Hill riot involved distrustful U.S. citizens attempting to overturn what they perceived as an illegitimate election, arguably the culmination of Russia and Iran's efforts.

4. Importantly, these cyber security incidents never passed the threshold of actually compromising the integrity of the US democracy by, for example, changing an electoral outcome. Rather, public trust in democracy was eroded by merely undermining the public's perception of legitimacy around the electoral process.

Australia's increasing exposure to cyber security risks

5. Australia is similarly targeted by autocratic nation-states. For example:

    - In early 2021, the People's Republic of China deployed its cyberwarfare capability to target vulnerabilities in the Microsoft Exchange email server. The breach purposefully enabled cyber criminals to access the emails of up to 70,000 Australian entities, including government organisations.[4]

    - It is reported that since 2018, Russia and the PRC have colluded in a social media misinformation campaign that has eroded public trust and impacted public health outcomes in

[2] Report of the Select Committee on Intelligence, United State Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1, Russian Efforts Against Election Infrastructure with Additional Views (2019). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.
[3] National Intelligence Council, Intelligence Community Assessment: Foreign Threats to the 2020 US Federal Elections (2021). Retrieved from https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.
[4] Doran, M. (2021), Criminals exploited Microsoft Exchange after China 'propped open the door', intelligence agency says. Retrieved from https://www.abc.net.au/news/2021-07-29/china-microsoft-exchange-hack-criminals-weakness-propped-open/100335008.

Australia.[5] The campaign was launched when Australia banned Chinese telecom corporation Huawei Technologies Co., Ltd. (**Huawei**) from building a 5G infrastructure network, and aimed to stoke public distrust toward the safety of 5G telecommunications infrastructure.[6] Sections of the Australian community are arguably still influenced by this interference, which has contributed to popular conspiracy theories around a purported relationship between 5G telecommunications technology and the coronavirus (**COVID-19**) pandemic, and fuelled misinformation around COVID-19 vaccines.

6. The Australian Cyber Security Centre (**ACSC**) reports that Australian entities were subject to approximately 67,500 cybercrime incidents in 2020-21,[7] a 13% increase from the 2019-20 financial year.[8] The ACSC—Australia's national cyber defence capability within the Australian Signals Directorate (**ASD**)—reports these incidents were predominantly committed by nation-state, state-sponsored and criminal actors. Victims included government organisations "at all levels" and critical infrastructure providers.

7. The ACSC attributes the rising trend in cyber security incidents to the high potential for state-actors to achieve cost-effective, zero-sum outcomes against Australian social cohesion and public trust by, for example, disrupting critical infrastructure.[9] Moreover, state-actors often sought sensitive information that could be used to degrade national security and essential service delivery.[10]

Case study – Reputational risk and the 2016 Australian Bureau of Statistics' e-Census event

8. The Australian Bureau of Statistics' (**ABS**) 2016 e-Census event demonstrates that a minor attack on a vulnerable information system used for carrying out an essential public service can cause major reputational damage and the erosion of public trust.

9. Although personal data was not stolen during the e-Census, the incident undermined the public's trust in the Commonwealth Government's ability to maintain cyber security and information availability when conducting an essential government service. #CensusFail trended globally over social media platforms, and ABS was unable to defer reputational damage onto IBM or ASD.

10. IBM provided the e-Census platform to ABS, and ABS looked to ASD to provide security assurance for the platform.[11] Despite ABS collaboration with IBM—one of the world's most experienced information technology companies—and ASD, on 'census night' the e-Census platform was affected by a distributed denial-of-service (**DDoS**) attack: a cyberattack involving the overloading of an information system with user requests, which prevents legitimate users from accessing the service.

11. The Special Advisor to the Prime Minister on Cyber Security incident report into the e-Census incident (**e-Census report**) indicates that ASD has limited resourcing capacity to service the need for cyber security across government.[12]

[5] ABC Four Corners, The Truth about 5G. Retrieved from https://www.abc.net.au/4corners/the-truth-about-5g/12519392.
[6] Ibid, number 5.
[7] The ACSC is the Australian Government lead agency for cybersecurity within the Australian Signals Directorate.
[8] Australian Cyber Security Centre (ACSC), Annual Cyber Threat Report 2020-21. Retrieved from https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21.
[9] Ibid, number 8.
[10] Ibid, number 8.
[11] Alastair MacGibbon, Special Adviser to the Prime Minister on Cyber Security, Review of the Events Surrounding the 2016 eCensus: Improving institutional cyber security culture and practices across the Australian government (13 October 2016). Retrieved from https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22publications/tabledpapers/a41f4f25-a08e-49a7-9b5f-d2c8af94f5c5%22.
[12] Ibid, number 9.

12. Additionally, the e-Census report suggests that the communications between ABS, ASD and IBM preceding the incident indicate a lack of clarity in capacity, roles and responsibility for cyber security across government agencies and contracted service providers.[13]

13. The e-Census report also highlights that a DDoS attack was a foreseeable threat that could have been mitigated by remediation of security architecture vulnerabilities in the e-Census platform. These were:[14]

    a. Controls were not considered within a comprehensive security framework;

    b. Risk assessments underestimated the consequences of security incidents, leading to insufficient focus on mitigation of risk; and

    c. Poor independent assessment and verification of security arrangements.

Transparency in the electoral process

14. When the public can physically observe and verify the legitimacy of electoral processes, the perception that the electoral process is legitimate cannot be easily undermined. For example, during the vote polling process, electoral security is visible to any constituent who stands in an election room and watches the polling unfold. The constituent witnesses an official poll clerk supervising voters marking their names off from an electoral roll, being presented with a printed ballot paper, and entering a private polling booth: all under the supervision of a poll clerk.[15]

15. If representatives of a rival nation-state were to walk into a polling station and attempt to steal, erase, or change the details of the electoral roll, public witnesses would physically observe polling officials countering the threat. Such a perceptible security measure maintains the public's trust in the integrity of the election because public witnesses can visually verify the success of the mitigation.

16. In contrast, demonstrating the integrity of any digitised electoral process is inherently more difficult than observable, in-person verification. For example, if a cyber incident occurred that altered or modified the information on an electoral roll, proving or verifying the roll remains uncompromised may be difficult.[16]

17. Democratic jurisdictions, including parts of the US, that have not adopted secure and transparent electoral processes have experienced decades of troubled elections.[17] As was observed in the most recent US presidential election, the mere perception that electoral processes have been compromised is sufficient for stoking socio-political tension and undermining public trust in the liberal social contract.

18. Integrating transparency and verifiability as a design goal of any future electoral roll is critical to ensuring trust and confidence is maintained.

Third party IT supply-chain solutions

19. The ACSC has stated that IT supply-chain compromises, as occurred against the Microsoft Office email exchange in 2021, are now the "new norm". Indeed, ACSC reported that state-sponsored actors and

[13] Ibid, number 9.
[14] Ibid, number 9.
[15] Teague, V. Keyzer, P. (2020), Electronic Australian Elections: Verifiability of Accuracy is a Design Goal, which Must be Mandated by Law and Deliberately Designed into Electronic Electoral Processes. 37(1):42-5. Retrieved from https://journals.latrobe.edu.au/index.php/law-in-context/article/view/119.
[16] Ibid, number 13.
[17] Ibid, number 13.

cybercriminals were able to rapidly exploit vulnerabilities to breach Australian entities at scale by targeting IT supply-chain providers on multiple occasions over 2020-21.[18]

20. Should a future electoral roll be underpinned by a third party commercial-off-the-shelf solution, electoral commissions must be aware of and manage the risks highlighted by the events of 2020-21.

Invulnerable systems do not exist

21. Even if a future electoral roll relies on purpose-built software, significant risks to the integrity of the systems hosting the electoral roll remain. As mentioned earlier, there are several nation-states with an interest in destabilising democracy in nations like Australia. These nation-states, and many other developed nations, stockpile and deploy offensive zero-day exploits.[19] A zero-day exploit describes an offensive capability that has been built to exploit a software security vulnerability, which the software developer has failed to identify.

22. At an opportune moment, nation-states can deploy a stockpiled zero-day exploit to infiltrate, alter or degrade target systems, including software, servers and network hardware. Such a moment might include, for example, an election event. The actual exploits can be carried out by state-sponsored actors, who are often for-hire businesses that are, or appear to be, at arm's length from the nation-states themselves.[20] Effectively, this means that an information system can never be completely protected from a motivated and well-resourced attacker.

23. OVIC encourages VPS entities to prioritise mitigation strategies and to ensure appropriate defences protect critical information assets. However, VPS entities must be aware that some vulnerabilities cannot be fully eliminated. Therefore, incident response plans and rehearsed incident responses should be implemented.

Best practice regulatory strategies

Ensuring a mature cyber security function is protecting electoral roll information systems

24. The ACSC within ASD is Australia's most mature cyber security agency and has a strong reputation among Australia's international partners. As a member of Australia's Intelligence Community, the ACSC is most equipped for defending Australia against the cyberwarfare capabilities that are increasingly being deployed against democracies by autocratic nation-states. As such, decision making around the future of a national electoral roll platform would benefit from consultation and ongoing collaboration with ACSC.

25. Integrating the Victorian electoral roll into a single, defendable national platform could improve ASD's capacity to defend critical infrastructure systems, as opposed to allocating a spread of operational resourcing across disparate information systems.

A comprehensive information security framework

26. The confidentiality, integrity and availability of any electoral roll platform would be enhanced by being subject to a comprehensive, legislated information security framework that reflects international best practice standards.

[18] Ibid, number 8.

[19] Maxwell, P. (2017), Stockpiling Zero-Day Exploits: The Next International Weapons Taboo, in Bryant, A, Mills, R, Lopez, J (eds.), *Proceedings of the 12th International Conference on Cyber Warfare and Security*, (9 February 2017) ISBN: 978-1-5108-3790-4, (pp. 237-243). Academic Conferences and publishing limited, 2017.

[20] Howell O'Neill, P. (September 2021). 2021 has broken the record for zero-day hacking attacks. MIT Technology Review. Retrieved from https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons.

27. As noted at the beginning of this submission, Victoria is currently the only jurisdiction in Australia with a legislated information security framework (**the VPDSF**) and standards (**the VPDSS**).

28. The VPDSF provides direction to VPS entities, such as VEC, on their information security obligations. Reflecting the public sector's unique operating requirements, it builds security risk management capability and maturity using existing international best practice risk management principles and guidelines. The VPDSF is complemented by the VPDSS, which consists of 12 high-level mandatory requirements to protect public sector information across all security areas including governance, information, personnel, information communications technology, and physical security.

29. OVIC, as an independent, statutory regulator monitors and assures the application of information security controls across VPS entities. This monitoring and assurance program ensures that the information security claims made by VPS entities are tested, validated and verified.

30. Conversely, Commonwealth agencies self-report compliance against a protective data security framework that is not legislated, nor subject to independent monitoring. The absence of a legislated information security framework in the Commonwealth, as well as independent regulator, may undermine the application of information security controls.

Thank you again for the opportunity to make a submission on the Inquiry into whether Victoria should participate in a national electoral roll platform. I have no objections to this submission being published without further reference to me. I also propose to publish a copy of this submission on the OVIC website, but I would be happy to adjust the timing of this to allow you to collate and publish submissions proactively.

If you would like to discuss this submission, please do not hesitate to contact me directly or my colleague Luke Whitehand-Willick, Senior Policy Officer, at Luke.Whitehand-Willick@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
Information Commissioner