



GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

Meeting Minutes – Online Voting

Date:	7 th November 2019
Time:	1400-1530
Attendees:	<p>Auckland Council:</p> <p>Marguerite Delbet</p> <p>Jenny Bolton</p> <p>Kieran O’Callaghan</p> <p>Warwick McNaughton</p> <p>DIA: (via conference phone)</p> <p>Scott Wilson</p> <p>Amanda Shaw</p> <p>Matt Walker</p> <p>NCSC:</p> <p>Jan s6(a)</p> <p>Ben s6(a)</p> <p>s6(a)</p>
Apologies:	Mark Denvir

Released under the Official Information Act 1982

Current Situation

Marguerite provided a summary of what had occurred so far towards online voting and their intent going forward.

Actions so far:

- Recognised the need for voting transformation. Current system numbers trending down and low youth engagement.
- Nine council partnership, led by Auckland to investigate online voting.
- Costs were and are to prohibitive for a council to go it alone.
- Worked with DIA throughout, acknowledged their error in not consulting GCSB. They wanted to at start but were unsure of how to. Also stated we had given some advice in 2016.

- They conducted a trial in December 2018 and pulled it due to not being ready by a set go/no go point.
- They recognised Identity management as a big sticking point.
- Authentication is also another big issue, they had developed a system with the help of a third party. Legislative restrictions at the time also did not help them.
- Acknowledged our stance on online voting, but they were taken by surprise by it.
- Stated the need for local and central to work together on this issue.
- Acknowledged PM support for local election online voting.

Marguerite provided a summary to the effect of: We now have the question of “how do we achieve online voting?” We know postal voting is no longer viable, other methods of in person voting are not viable. Online voting is a requirement and we see it as the way forward.

NCSC Summary of position

Jan provided an overview of the NCSC role and responsibilities. Jan and Ben then provided a summary of risks to online voting (as agreed upon prior in Ben ^{s6(a)}'s meeting notes). Key points included:

- Online voting being a topic of interest
- Reputational risk
- GCSB position on online voting
- Security concerns
- Risk based approach
- NCSC able to assist with questions as they arise

Discussion

Kieran asked what would constitute ‘good enough’ acknowledging the impossibility of a perfect system.

- Jan: Good enough would be very hard to achieve, and there is no set list of requirements.
- Ben: System end to end would need to be go through C&A.
- Jan: Talent to build such a system does not exist in NZ and those that could make it would not due to high level of risk.

Marguerite raised the point that online voting has been done elsewhere successfully which would imply it's possible to do properly.

- Jan: Case of Victoria University where their system was not secure and had multiple flaws.
- Ben: Australian experience so far has been ‘ok’ but there are lots of questions left unanswered.
- Marguerite: Disagreed saying that the media around the Victoria University case was sensationalist. There was a vulnerability however it was only at one level of security and the vulnerability was not exploited. Cautioned against allowing media to skew perceptions, these are not facts.
- Jan: Even so, Auckland Council would unlikely have the ability to create such a system.

Note added 3 Feb 2025:
References to Victoria University are an error and should be read to reference the case of the Australian state of Victoria using online voting technology.

- Marguerite: Acknowledged, stated that was why they had taken a combined approach with the nine councils.

Jan asked about who their third party providers were.

- Marguerite: Smartmatic were successful in the RFP process. Scytl only other real option. Smartmatic have world class cryptographers.
- Jenny: Smartmatic partnered with DATACOM, this was to enable smartmatic keeping the data in New Zealand.
- Marguerite: Data would always/have to stay in New Zealand.

Marguerite stated that their 2018 trial was unsuccessful largely due to running out of time. Therefore, they are starting the work now to be ready for the next election cycle. She stated that NCSC and Council's need to work together now to be ready. Marguerite further stated that they were in a state of democratic crisis with such low voting numbers and she acknowledged our concerns but they needed people to participate in the voting process.

Marguerite asked would we work with them to achieve online voting or would be continue to be against online voting.

- Jan: We exist to help all NSO's, Auckland Council included.
- Jan: We won't give a formal approval to an online voting system and even if we worked with you at the end of the process we may still object to online voting.
- We can provide a list of questions around third party considerations.
- We are not saying to not try, but right now we don't have confidence in any online voting system.
- Marguerite: Had NCSC looked at smartmatic and Scytl? And had the NCSC Estonia's online voting systems?
- Ben: Estonia have all the benefits of building a nation in the technology age. They have an integrated approach to identify management that does not exist here in New Zealand. Therefore, not a fair comparison.

- s9(2)(g)(i) [REDACTED]

Marguerite asked what the NCSC thought the objectives of an attacker would be.

- Jan: Stated that as mentioned earlier there are a number of attackers interested in a number of objectives.
- Marguerite: Asked if we have evidence to support Jan's statement.
- Jan: Yes, we will try to get some information released to you. This information was discussed by Andrew Hampton with a number of Mayoral Offices so Jan was confident it would be releasable.
- Warwick: A large issue was ensuring voter integrity and that the vote had not been tampered with. There are now systems to ensure this doesn't happen.
- Marguerite: The electoral role is public so there is already risk with voter integrity. This issue and all others would be discussed in detail if the NCSC agreed to work together.

Marguerite asked if the PM directed councils' to investigate online voting would we work with them?

- Jan: We would continue to offer our advice as we currently do. The level of prioritisation for us would depend on higher direction. If we were told to make

this a priority then we would have to. We would in any case require time to plan internally alongside other priorities.

- DIA person: Stated they would talk later with Auckland Council re Minister position on online voting.

Marguerite reiterated that this was note solely about Auckland Council, but all, specifically the nine in partnership.

- Jan: Asked who the nine were
- Combined answer:
 - o Auckland
 - o Wellington
 - o Tauranga
 - o Hamilton
 - o Gisborne
 - o Marlborough
 - o Selwyn
 - o Palmerston North
 - o Matamata


Jan agreed to look at the vendors in more detail for future feedback.

Meeting was closed.

END.

Recommendation-by-recommendation analysis: Justice Committee Inquiry into the 2017 General Election and 2016 Local Elections – comments from GCSB and NZSIS [27 January 2020]

Out of scope



Released under the Official Information Act 1982

Out of scope

Released under the Official Information Act 1982



Out of scope

Released under the Official Information Act 1982

#	Justice Committee recommendation	Information we have so far / initial thinking	Possible agencies	Further comments e.g. additional information, suggested response
Out of scope				
40	<p>We recommend that the Government retain manual or paper-based voting systems in local and general elections for the foreseeable future because of security concerns.</p>	<p>There is currently no known voting computer system architecture that would give an acceptable level of election security.</p> <p>There are no plans to move away from manual systems at the national level.</p> <p>Any incorporation of technology or online aspects to the electoral system must be very carefully managed.</p> <p>Security and integrity of the system are of the utmost concern.</p> <p>There is discussion in the local elections context around the difficulties with postal voting, but we understand that electronic voting is not a favoured solution to this issue.</p> <p>DIA – do you have thoughts on how you’ll deal with the response to this in the local elections context?</p> <p>Appearing before the Committee, GCSB’s Director-General said the GCSB has had ongoing concerns about the security implications of proposals to pilot or introduce online voting for local body elections.</p>	<p>GCSB</p> <p>DPMC (FI/cyber)</p> <p>DIA (local govt, GCDO)</p> <p>Electoral Commission</p>	<p>Support MoJ’s initial thinking on this recommendation.</p> <p>GCSB has ongoing concerns about the security implications of proposals to pilot or introduce online voting for local body elections. Manual voting is much less susceptible to compromise and the administrators of local elections do not have the experience or support that the Electoral Commission does.</p> <p><i>GCSB is interested to see the response from DIA to this recommendation.</i></p>
Out of scope				

NCSC's response to the draft Cabinet Paper, Report of the Justice Committee Inquiry into the 2022 Local Election

Overview

1. Thank you for the opportunity to provide feedback on both the draft Cabinet paper and the Government Response to the Report of the Justice Committee Inquiry into the 2022 Local Elections. Overall, we support the recommendations of the paper as it reflects that local government does not yet have systems in place that would support online voting.
2. Given the short timeframe, we have focussed our comments on the proposed trial of online voting in local elections (recommendation 3). Our feedback identifies important actions that would support the security and integrity for this proposal.
3. We are committed to working with relevant organisations to address cyber security concerns should there be further consideration of online voting options in local elections.

In summary

4. The NCSC is interested in exploring the potential of online voting and how robust security measures can be ensured at every stage of the process.
5. We consider that the following steps would need to occur to support the delivery of secure online voting:
 - a. An assessment of both threat and risk is completed, including supply chain risk, to inform the cyber security measures needed.
 - b. An uplift in cyber security expertise for those administering local elections. Clear roles and responsibilities are agreed for preventing and responding to incidents. We note that administrators of local elections would need to build their cyber security expertise. This would have to be addressed as part of any robust consideration of alternatives to the current local body electoral processes.
 - c. Systems would need to be tested and secured, including adoption of best practice cyber security controls. Any online voting system should align to government cyber security expectations and practice, such as the requirements of the New Zealand Information Security Manual.

More detailed feedback on Cabinet paper

Key considerations and steps to enable online voting could include:

6. Online voting could generate benefits but also introduce potential cyber security risks that could undermine the integrity of the voting process, and consequently the governance institutions. The benefits and risks of online voting should be evaluated against the status quo.
7. To ensure the security of online voting, the Government should undertake an up-to-date assessment of security risks and challenges. This assessment could then inform the nature of mitigations implemented.

Firstly, online voting has a different risk profile to other online activities and the impact of these risks need to be understood and appropriately mitigated

8. Cyber security considerations for election systems, namely, online voting, are different from other cyber security considerations. For example, online shopping and online banking have a higher tolerance of failure and are designed to tolerate such failure. If credit card fraud occurs or if sensitive personal data is breached, that is an economic cost that can be absorbed by the bank, merchant, or insurer. Breach of online voting could have far greater consequences, including undermining the integrity of democratic processes. It is difficult to “make voters whole again” after a compromised election.
9. Additionally, elections could be high-value targets for sophisticated nation-state attackers. Nation-states may interfere with our elections to merely undermine the confidence of its outcome. While we recognise that the proposal for online voting considers a trial for local body elections only, it is necessary to carefully consider the threats and risk that local government processes face and how this might provide an opportunity for attackers to use this as a test case. Due to local governments role in resource management, critical infrastructure ownership and community support we cannot rule out state sponsored cyber threats.

Secondly, the threats to online voting systems need to be evaluated and analysed

10. Online voting could introduce several cyber security threats, including, but not limited to:
 - Compromise of a device’s hardware and/or software, possibly via supply chain attacks,
 - Failing to properly record a voter’s choices,
 - Tabulation errors,
 - Corruption of evidence trail,
 - Ballot “stuffing” (extra ballots) or ballot destruction.

Finally, like any online system, online voting systems are vulnerable to cyber attacks and theses vulnerabilities need to be identified

11. Cyber security is complex, with criminal, state, and non-state actors using attacks to achieve their aims. Vulnerabilities could be exploited by attackers at different

points in the process. For example, attackers can exploit the device used to cast votes. More specifically, attackers can modify a computer's hardware, software, or equipment and gain access to information or change the system's operation. This means that attackers could have complete control over targeted voting systems and how they interact with the voter. Attackers may disrupt the casting and tallying of votes, or deceive voters about any aspect of the voting process.

12. For instance, in 2015, New South Wales (Australia) deployed online voting, namely the iVote System, to conduct its state elections. During the election, an independent team conducted a security analysis of the iVote System. They found that a network-based attacker could perform an attack to compromise ballot privacy and steal online votes. While there is no evidence to suggest that anyone exploited this security flaw, the opportunity to exploit it was there.

13. Furthermore, flaws in the voting system may be introduced by the voting software vendor, the hardware vendor, the manufacturer, or any other third party that maintains or supplies the code for these organisations that manage online voting. Understanding and managing supply chain risk will be important.

Considerations when establishing a safe and secure online platform for voting

14. Like any good voting system, an online voting system requires secrecy (so voting can be anonymous); integrity (so votes are recorded correctly); and verifiability (so doubters can check votes are recorded correctly, persuading those who doubt).

Secrecy

15. Officials would need to determine how to safely and securely authenticate online voters, while ensuring that ballot secrecy is maintained.

16. Cyber security measures would need to be put in place to ensure that hackers do not intercept information being transmitted to the voting server and learn how an individual voted.

Integrity

17. Digital electoral processes would need to be resistant to cyber attacks. Given the complexities of the Single Transferrable Voting system, and the possible avenue for judicial review of results, a vote counting process would need to be a high integrity process capable of being audited and understood.

Verifiability and assurance

18. It may be difficult to assure the integrity of online voting results because exploitation is often undetectable to users and a forensic examination of the device may not reveal its presence. Verification of online voting results will likely rely on expert testimony, rather than a manual count.

19. Finally, there are some promising methods for online voting, but any implementation would need to be carefully designed, well implemented, closely monitored, and assured at every step of the process.

Next steps:

20. We appreciate the opportunity to provide input on the Cabinet paper.

21. We consider that the suggestion of foreign interference, voting manipulation, or human error in the design of an online voting system could lead to loss of confidence in New Zealand election results and therefore undermine our democratic processes. As this work progresses, we welcome further engagement with NZSIS and GCSB.

22. A threat assessment and a risk assessment are critical inputs for designing a safe and secure online voting solution. NCSC recommends that a threat assessment and a risk assessment are completed to enable the Minister of Local Government, Secretary of Local Government, and local authority decision makers to understand the cyber threats facing local elections, and discuss how best to set appropriate risk tolerances for an online voting solution.

23. Should DIA and the local government sector undertake further work on online voting, NCSC would seek to engage to ensure cyber security concerns are addressed and well managed.

Online voting

Taituara | Local Government Professionals' Elections Reference Group is considering online voting for the next local government election.

How we'll talk on Friday:

1: Threatscape and strategic context [Leah]

Election related cyber espionage:

- Internationally, election-related cyber espionage has targeted accounts, networks, data repositories, and communications platforms associated with government organisations, political parties, individual candidates, news/media outlets, political activists, academic institutions, and lobbying groups.
- Overseas, councils have experienced numerous cyber security incidents, including ransomware and limited-impact DDoS affecting information websites belonging to councils.

Key points pre-LGE2022:

- At the outset of the event, the NCSC assessed there to be a realistic possibility that malicious cyber activity – including that which may have been unmotivated by the election – could impact organisations and local councils during the LGE2022 period.
- Local councils are occasionally a target for sophisticated malicious actors.
- Furthermore, the NCSC assessed there to be a realistic possibility of current undetected compromise on an organisation's network.
- In the context of LGE2022 the vector of compromise assessed to have the highest impact was almost certainly a supply chain compromise. A malicious cyber actor may have sought to compromise a common supplier to have a widespread impact on the election.
- Malicious cyber actors, including those of moderate capability, almost certainly have the ability to compromise personal devices, which may then be used to infiltrate a council network.
- Malicious actors may target councils or their contractors to acquire electors' personal information, or cause limited-impact DDoS affecting information websites belonging to

councils. Other malicious actors may take advantage of the heightened awareness of election activity to conduct low level cyber crime.

Key points post-LGE2022:

- In the Local Government Elections 2022, the NCSC did not observe any cyber targeting, nor intelligence to suggest an intent to target via cyber means, the event.
- The paper based nature of the event highly likely reduced the threat surface, and the disaggregated nature of the event almost certainly reduced the opportunity to influence or disrupt the process overall.
- What the NCSC did observe is occasional scanning and reconnaissance activity, which is consistent with opportunistic targeting of internet facing services.
- Outside of the context of the Local Government Election 2022, the NCSC were aware of incidents affecting the networks of local councils.

Cyber threat to local government, international perspective:

- Over recent years international insights have identified the risk posed to local government organisations more widely, and the realistic possibilities of experiencing loss (both financial and data), business impact, and reputational damage as a result of malicious cyber activity.
- Local governments overseas are assessed to be even more likely a target for malicious actors than federal or state agencies.
- Whilst, internationally, some local governments are recognised to be investing more in cyber resilience, this has not always materially improved the risk profile alongside the rate of threat environment change. Risk management and effective resilience are recognised as key to helping to prevent malicious cyber incidents.

2: NCSC position on online voting [Ben]

NCSC Key messages from December 2022

- Any discussion of online voting for local body elections needs to carefully balance considerations around access and participation with risks to the security and integrity of the process which could be introduced.
- A move to online voting would need to build in robust security at every stage of the process. Even the suggestion of an instance of vote manipulation, or human error in the design of an online system, and the whole result would be subject to questions.
- Effectively addressing the security risks associated with online voting requires a high level of cyber security maturity.
- s9(2)(g)(i) [Redacted]
- We are committed to working with relevant organisations to address cyber security concerns should there be further consideration of online voting options in the future.

Released under the Official Information Act 1982



3: Recommendations for EWG

1. **Update the threat assessment from 2016 for the current environment.** To be realistic, that threat assessment should assess and deal with a full range of threat actors – insiders (the malicious and the incompetent), issues motivated groups (heightened risk compared to 2016), criminal groups, nation state actors). Share the threat assessment across relevant stakeholders to everyone is operating with the same assumptions.
2. **Plan for a longer implementation period:** the last 9 years have seen the sector try and implement online voting for the next election, and it hasn't worked yet. If you are serious about making this work, our advice would be that the challenges are significant and need a longer runway and project timeframe than a single electoral period.

Recommendations from 2016 Cabinet decision

Recommendations for way forward

Cabinet noted the recommendation to:

- a) **Engaging the voting community:** As per the advice on the Online Voting Working Party, local government should be seeking to run staged implementation whereby communities can become familiar with the online voting system through:
 - Organising workshops to help people share their views and show them the online voting systems. •
 - Non-binding trials such as referenda and mock elections (this is international best practice). •
 - Using the system in small-scale politically binding trials such as by-elections. •
 - Trial the technology in selected sites.
- b) **Engaging the technical and academic communities:** The technical and academic communities can provide considerable help to an online voting trial. Their confidence in the confidentiality, integrity, availability and privacy of the online voting system will be critical to ensuring successful use of online voting systems. Suggestions include:
 - Organising workshops to help people share their views and discuss how different groups and parts of the community can be involved in making online voting a success. •
 - 'Open sourcing' online voting system source code so that academic research teams and open source advocates can review and contribute to the betterment of the software.
 - Running a bug bounty, enabling New Zealanders to contribute to the security of the online voting.

Things that had not been done at the point the project was stopped back in 2106 included:

- independent review of the source code for voting systems;
- whole-of-system penetration testing;
- independent assurance of key aspects of the trial requirements
- development of a detailed coordinated national communications strategy.