

Julienne Molineaux
The Policy Observatory
Auckland University of Technology
julienne.molineaux@aut.ac.nz

Dear Julienne

Official Information Act 1982 request OIA1819-0548

Thank you for your request under the Official Information Act 1982 (the Act) received by the Department of Internal Affairs on Monday 11 March 2019. You requested:

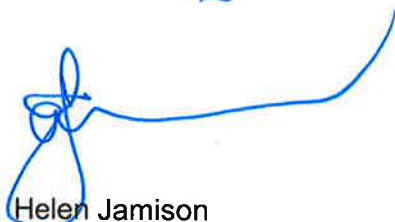
- Any advice or input (including technical or security) your Office or its staff gave on the proposed online voting trial for the 2019 local government election, whether to the Department of Internal Affairs or any local territorial authority or a Minister or anyone else.

Copies of the documents that come within the scope of your request are attached. Some information has been withheld and, where this is the case, the relevant section of the Act is provided. Within the documents I am withholding information where it is necessary, to protect the privacy of natural persons, subject to section 9(2)(a) of the Act.

Please note that copies of the paper "Modernising voting – security recommendations for online voting for local elections", draft Cabinet paper "A regulatory approach to enable local government online voting trials in 2019", "Requirements for a trial of online voting in local elections" have been included in this release: they are provided to give you context for the comments but are not documents that were produced by the office of the GCDO.

If you are dissatisfied with this response, you have the right to seek an investigation and review of this decision by an Ombudsman under section 28(3) of the Act. The contact address is: Office of the Ombudsman, PO Box 10152, Wellington 6143. You can also phone 0800 802 602 or send an email to info@ombudsman.parliament.nz.

Yours sincerely



Helen Jamison

General Manager, Strategic Relationships and Advice

From: 9(2)(a)(a)
Sent: Tuesday, 24 October 2017 6:50 PM
To: 9(2)(a)
Cc: 9(2)(a) 9(2)(a) 9(2)(a)
Subject: RE: Modernising voting - Expertise on

Hi 9(2)(a)

Many thanks for passing these on. I'm just having a first read through these now, and also passed them to our new security specialist 9(2)(a)(a) (cc) who started with us today. 9(2)(a) will be helping in this work, but for now I should probably stay as your main point of contact.

As noted, this is from preliminary reading only, but first up, I see that the 2015 requirements are based on the Council of Europe 2004 recommendations Rec(2004)11 which have been revised significantly this year on the basis of the last 13 years' developments and experience.

For requirements to be useful in an RFP, it goes without saying that they should be (amongst other things):

- Meaningful
- Quantified / measurable where possible
- Achievable
- Consistent

I'm not sure that some of the requirements (e.g. 2.53) are worded in a way that meets these goals. Perhaps they could be pitched as considerations for local authorities when they are writing requirements, rather than things for them to quote verbatim. Perhaps for further clarity it might also be useful to follow the EU example and provide a glossary and a supplementary paragraph or two that explains the rationale and implications for each requirement.

It will also take some careful reading to ensure that some of the requirements aren't mutually exclusive. Some ideals in an electronic or internet voting system usually have to be traded off, e.g.

- 1.4 vs 2.33-34 (no pre-registration required, but authentication & identification required). I suppose this depends on the meaning of "pre-registration". Presumably voters have to be on the roll as per the Local Electoral Act?
- 1.22, 1.23 vs 1.24 and others relating to receipt-freedom. Requirements 1.22 and 1.23 seem to have been added by NZ, whereas other jurisdictions allow a "last vote counts" policy to allow the implementation of a receipt-free system.

Finally, (2.58) I'm not sure that any of our Security and Related Services panel in NZ (let alone a council ICT unit) would have the specialist technical knowledge to validate an implementation of an online voting scheme that is subject to the supplied requirements. As we noted in 2014/15, this is a specialised and contentious area where we would recommend some international / academic expertise, both in the framing of the requirements, and in the assurance of the implementations.

I will keep reading ... can you let me know when a final response is needed please?

Thanks,

9(2)(a)

From: 9(2)(a)
Sent: Tuesday, 24 October 2017 2:01 p.m.

To: 9(2)(a)

Cc: 9(2)(a)

Subject: Modernising voting - Expertise on

Hi 9(2)(a)

Can I please check with you on the best point of contact for some advice on security and assurance service level targets for the online voting trial in local elections?

We are working with the local government sector representatives to review the 2015 Requirements to check that they are still fit for purpose. The intention is that some of these requirements will be the basis for regulations for online voting trials, and that others will be part of the Service Level Agreement that councils will have with the online service provider.

The sector has asked us to seek SST/GCIO input on the following:

- advice on whether the security requirements (Requirements 2.53 – 2.56) are still up to date and reflect best practice
- whether Requirement 2.22 (which prevents vote and voter information being transmitted or held outside NZ) is still required or whether the cloud-related Requirements (2.59 and 2.60) are sufficient
- attending the next Expectations working group meeting. [LGNZ and SOLGM are inviting representatives from InternetNZ and the Association of Local Government Information Management (ALGIM) to attend the meeting to discuss security and assurance and they are keen to have someone from DIA with expertise in this area attend also. The workshop is on Wednesday 1 November from 11 3pm. I would anticipate that this agenda item could be 1.5 2hrs but SOLGM have said they are happy to be flexible about where on the agenda this item is to help work around diaries.]

On the issue of information being held overseas, 9(2)(a) has put us in touch with 9(2)(a) and we're going to catch up with him about that.

On the other matters are you the best point of contact?

Thanks,
9(2)(a)

9(2)(a) | 9(2)(a) | 9(2)(a)
The Department of Internal Affairs Te Tari Taiwhenua
Direct Dial: 9(2)(a) | 9(2)(a) | Level 7

From: 9(2)(a)
Sent: Tuesday, 11 December 2018 5:29 PM
To: 9(2)(a) 9(2)(a)(a) 9(2)(a)
Cc: 9(2)(a) 9(2)(a)(a)
Subject: RE: FYR online voting party notes

Sorry – forgot to answer the second question.

9(2)(a) – were these the security recommendations, and were they passed to the Working Group?
https://dia.cohesion.net.nz/sites/TEA/GEA/_layouts/15/WopiFrame.aspx?sourcedoc={338DBD1D-B52A-439C-AFC3-5D27517FC0B4}&file=Modernising%20Voting%20-%20Draft%20Security%20Recommendations.docx&action=default&DefaultItemOpen=1

Or were they incorporated into other documents passed to the group?

There was an early discussion with the DIA team on the subject of the “last vote submitted” option, but I think it was omitted from the final recommendations as the Local Electoral Matters Bill was already too far advanced.

One other addition was under point 3.3, third bullet: Smartmatic and the programme agreed that the voting procedure and the system source code would be made available to academic scrutiny under appropriate NDA protection, if I recall correctly.

From: 9(2)(a)
Sent: Tuesday, 11 December 2018 4:13 PM
To: 9(2)(a) 9(2)(a)(a) 9(2)(a)
Cc: 9(2)(a) 9(2)(a)(a)
Subject: FYR - online voting party notes

Hi

Thanks for attending last Friday’s meeting on authentication and online voting.

Attached are my typed up my notes – could you please include any significant points from your notes I have missed or let me know if I have incorrectly captured anything.
If possible, could you do this by COP tomorrow so I can circulate the notes to other participants.

9(2)(a) – is the attached EOI risk assessment the earlier work you referred to during the meeting?

9(2)(a) – What document did you refer to that could be provided to the Working Party?
Was it the draft security recommendations?
https://dia.cohesion.net.nz/sites/TEA/GEA/_layouts/15/WopiFrame.aspx?sourcedoc={338DBD1D-B52A-439C-AFC3-5D27517FC0B4}&file=Modernising%20Voting%20-%20Draft%20Security%20Recommendations.docx&action=default&DefaultItemOpen=1

Thanks

9(2)(a)

9(2)(a)

From: 9(2)(a);(a)
Sent: Monday, 30 April 2018 9:07 PM
To: 9(2)(a)
Subject: Modernising voting security paper

Hi 9(2)(a)

I've saved the paper [here](#). I've added some preamble about the assumptions having changed and the need to review once new expectations are understood. Otherwise it's still base don the old assumptions, though I don't think it changes much.

Regards,

9(2)(a);(a) | 9(2)(a) – 9(2)(a)
Te Kōtahi Whiriwhiri | Service & System Transformation (SST)
9(2)(a) | www.dia.govt.nz

Released under the Official Information Act 1982

Modernising Voting – Security Recommendations for Online Voting for Local Elections

Released under the Official Information Act 1982

Contents

Introduction	3
Constraints and Assumptions.....	3
Key Objectives for Online Voting	3
Objective 1. Public Confidence	4
Objective 2. Accessibility.....	4
Objective 3. Accuracy.....	4
Objective 4. Equivalence with current system.....	5
Delivery Recommendations	6
Recommendation 1. Project scope and resource	6
Recommendation 2. Subject Matter Experts.....	6
Recommendation 3. Consultation	7
Recommendation 4. Reassess Information Classification	8
Recommendation 5. Integration into current election processes.....	8
Recommendation 6. Consider applicability to future elections	8
Security Threats and Requirements	9
Threat Categories	9
Threat Descriptions	10
High level Security Requirements	12
Appendix A Conceptual model	16
Appendix B Service Levels and Availability	17
Appendix C Past Recommendations	18
Appendix D References	19

Introduction

These recommendations are based on the knowledge gained from a high level overview of the current local election process, documentation from the investigation of online voting feasibility and discussions with the Modernising Voting Working Group. Key documents are referenced in Appendix D.

This document gives two sets of recommendations:

1. Recommendations for delivery ,
2. An initial analysis of security threats to online voting, and requirements to address those threats.

Constraints and Assumptions

At the time of preparation the Modernising Voting Expectations Group had specified the following constraints and assumptions for the trial of online voting in 2019. Since the preparation of this paper the expectations for both the delivery approach and timelines have changed. Once the new approach and timelines have been established this paper will need to be reviewed and updated.

These constraints and assumptions upon which this paper has been based are:

- A single online voting service provider will be selected.
- The online voting solution will exist alongside current postal voting service providers, and will be responsible for securely collecting online votes.
- The existing election service providers will be responsible for counting online votes alongside the postal ballot.
- The 2019 local election online voting trial will put in place the necessary capabilities and functions to support the trial, and will not be delivering all of the capabilities necessary for future online local elections, parliamentary elections or referenda.
- The working group is expecting that the content of the electronic ballot box will be decrypted and printed in a form that can be scanned and counted by the existing election service providers using their existing facilities.

Key Objectives for Online Voting

The Local Electoral Act¹ has three core principles² which must be reflected in the Online Voting solution:

- **Fair and effective representation** for individuals and for communities,

¹ <http://www.legislation.govt.nz/act/public/2001/0035/latest/whole.html>

² [https://www.dia.govt.nz/vwluResources/Reqs-for-trial-online-voting-in-local-elections-Nov15-docx/\\$file/Reqs-for-trial-online-voting-in-local-elections-Nov15-docx.docx](https://www.dia.govt.nz/vwluResources/Reqs-for-trial-online-voting-in-local-elections-Nov15-docx/$file/Reqs-for-trial-online-voting-in-local-elections-Nov15-docx.docx)

- All qualified people have a **reasonable and equal opportunity** to cast an informed vote to nominate a candidate and to become a candidate,
- **Public confidence** in local electoral processes and public understanding of local electoral processes including:
 - protection of the freedom of choice of voters and the secrecy of the vote,
 - transparent electoral systems and voting methods, and
 - certainty in electoral outcomes.

Objective 1. Public Confidence

Arguably the most critical objective for the trial is to build public confidence – at a minimum not to damage public confidence – in online voting as part of New Zealand's democratic processes. To ensure public confidence it is important not only that the Online Voting solution upholds the core principles, but that it is also *seen* to uphold them.

Any perceived failure of the Online Voting trial is likely to severely damage any future attempts to introduce online voting. This would likely affect online voting in other democratic processes such as general elections or referenda. It is critically important that the trial is well planned, well-resourced and of high quality.

It is also necessary to consider that a newly introduced online voting system can be expected to fall under closer scrutiny than the current established electoral processes. It is likely that this scrutiny will come from sources both nationally and internationally, both benign and hostile to New Zealand's interests.

Objective 2. Accessibility

Online voting opens new ways to provide reasonable and equal opportunity to electors who may have difficulty with the postal system, such as those living in remote areas or overseas, or where voters require assistance completing their vote because of physical impairment or other needs. Online voting can work across geographical boundaries and can be used with assistive technology like screen readers and input devices.

When considering security requirements for the solution we must also consider how these requirements might affect the accessibility and usability of the solution. Where compromises need to be made the reasoning and justification for the decision must be documented clearly and openly.

Objective 3. Accuracy

It is important that the final count accurately reflects the intention of the electors. The postal ballot system is unable to provide checks and feedback to help the voter make sure that the vote cast is what they intended. This can be particularly seen in STV elections where high rates of informal votes are received.

Objective 4. Equivalence with current system

Voters participating in the online voting trial will have the option of voting online or through postal voting. Both options should allow the elector to vote for the same issues, present the same information about candidates, and provide means for an elector to spoil their ballot.

An example of providing equivalence while still delivering desirable benefits from online voting could be an elector submitting a protest vote by spoiling their ballot. In the postal ballot system an elector can submit a blank ballot or mark their ballot in a way that makes it invalid. Online voting provides opportunity to advise electors if they are about to submit an invalid ballot, but should provide means for an elector to leave their ballot blank, invalidly mark their ballot, and must not prevent such a spoiled ballot from being submitted. This would reduce the likelihood of a ballot being spoiled accidentally, without affecting an elector's choice to submit a deliberately spoiled ballot.

Released under the Official Information Act 2002

Delivery Recommendations

A working party was established in 2013 to investigate the feasibility and options for online voting in New Zealand. The working party published its report in 2014, giving 20 high level recommendations. Security recommendations from the 2014 report are summarised in *Appendix C, Past Recommendations*.

The recommendations presented in this report are focussed on those needed to deliver a secure, reliable solution for trailing online voting for local body elections, and one that meets the key objectives.

Recommendation 1. Project scope and resource

In order to ensure that the online voting solution is reliable, trustworthy and secure it is important that the specification and delivery of the solution is well planned and well governed. We recommend that the project scope includes:

1. Establish **agreed objectives** for the online voting trial. What do local government bodies and central government **want to learn** from the implementation and execution of the trial?
2. Establish **clear ownership and accountability** for the objectives, risks, implementation and operation of the solution.
3. Updated **market analysis**³ of online voting service providers and solutions, taking into account changes in approach and objectives since the work done prior to the 2016 local elections.
4. Complete a comprehensive **risk analysis** of both project delivery risk and the ongoing risks of operating online elections. As there is very little historical data to support an analysis of the likelihood of serious incidents affecting online electoral processes, risk analysis should focus on identifying **threats** to public confidence in online and electronic voting, and the **potential consequences** if those threats are realised.
5. More detailed **requirements analysis** focused on **business requirements and objectives** rather than technical requirements. The options for **integration** of the online voting solution with the existing election service providers should be assessed.
6. **Consultation** with the wider community to give the solution the best chance of public acceptance of online voting.

Recommendation 2. Subject Matter Experts

The project team should closely engage with subject matter experts in online voting systems and cybersecurity. Due to the criticality of cybersecurity to the success of the solution and the likelihood that other decisions could have security impact we recommend that a cybersecurity expert is included in the core project team. We suggest that other subject matter experts could include:

³ <https://dia.cohesion.net.nz/Sites/GCIO/AOGA/ReferenceLibrary/Online%20voting%20-%20Early%20market%20engagement%20report%20v0.1.pdf?Web=1>

- An independent subject matter expert with experience in the implementation of an online voting solution, such as the NSW iVote implementation.
- A representative from Stats NZ familiar with the implementation of the Online Census.
- A representative from the NZSIS and/or GCSB to provide advice about electronic threats and risks.

Recommendation 3. Consultation

It is likely that the introduction of online will bring close scrutiny from both domestic and overseas sources. A notable example of this is the Paris town hall primary election of 2013⁴ during which journalists successfully interfered with the electoral process, voting multiple times using different names. This can affect public confidence in the system even if it can be demonstrated that there has been no material impact to election outcomes.

Consultation with representative and community groups is recommended to improve public confidence in the solution. Consulting with representatives of the wider community will not only help to deliver the best possible solution for online voting, but will address community concerns early in the process and increase the likelihood of public acceptance of online voting for the 2019 local elections.

The baseline expectation is that the online voting solution must be no less secure than the existing postal system. If the online voting system is to come or close scrutiny or is challenged in some way this may not be sufficient to maintain public confidence in the system.

Consultation could include a wide range of groups such as InternetNZ, political academic researchers, and representatives of the Māori, Pacifica and other New Zealand cultural communities.

⁴ <http://www.independent.co.uk/news/world/europe/fake-votes-mar-france-s-first-electronic-election-8641345.html>

Recommendation 4. Reassess Information Classification

The requirements for trial online voting⁵ documented in 2015 recommended that systems delivering online local elections are secured to a level appropriate for information classified as "In Confidence." No reasoning for this requirement was documented. We recommend that this classification is reviewed. The inappropriate disclosure of voter and vote information in a single local election may well have consequences consistent with an "In Confidence" classification; however disclosure of this information on a national scale may have consequences justifying a higher classification. Classification higher than "In Confidence" would require a review of the requirements, including security requirements, and could limit the options available to meet those requirements. In particular this could mean that the online voting solution may need to be hosted and operated within New Zealand borders.

Recommendation 5. Integration into current election processes

There should be more detailed consideration of the options and feasibility of integrating potential online voting solutions with existing electoral processes and systems.

Integration of systems often requires substantial design, implementation and testing effort. This is especially so when the integrity and confidentiality of the data being integrated is of critical importance. In a previous market analysis of online voting solutions in 2014 the current New Zealand election service providers indicated that they believed integration with a third party online voting service to be risky.

In order to reduce the effort and cost of integrating the online voting trial solution with existing systems, the Modernising Voting Expectations Group has proposed that the electronic ballot box can be decrypted and printed for processing by the election service providers. It is not clear that this will avoid the need for some level of integration; it will still be necessary for the electronic ballot box to be securely transferred from the online service provider to the election service providers either digitally or once printed.

Recommendation 6. Consider applicability to future elections

Consideration should be given to future uses of online voting when defining learning objectives for this trial.

The approach taken by the modernising voting expectations group has understandably focussed on the requirements for running a trial of online voting in the 2019 local elections.

It is likely that a well-designed trial will provide insights into the use of online voting in parliamentary elections and referenda as well as local elections. It is also possible that compromises made to meet the time and cost constraints for this trial could reduce the opportunities for learning, and could even result in a solution which is not suitable even for future local elections.

⁵ [https://www.dia.govt.nz/vwluResources/Reqs-for-trial-online-voting-in-local-elections-Nov15-docx/\\$file/Reqs-for-trial-online-voting-in-local-elections-Nov15-docx.docx](https://www.dia.govt.nz/vwluResources/Reqs-for-trial-online-voting-in-local-elections-Nov15-docx/$file/Reqs-for-trial-online-voting-in-local-elections-Nov15-docx.docx)

Security Threats and Requirements

This threat analysis is based on a conceptual model for online voting described in Appendix A. This analysis is not exhaustive. A more detailed threat and risk analysis must be performed by the trial implementation project. The consequences described below apply before mitigating controls are put in place.

Threat Categories

The identified threats fall into several high-level categories:

Threat Category	Description
Voter coercion	Both postal and online voting are undertaken without official oversight and the threat is similar in both cases. No special treatment of this threat is required for the online voting trial. If the solution is expected to extend to parliamentary elections this will become a consideration.
Interception or manipulation of votes	The opportunities for a malicious party to intercept or manipulate votes individually or en masse are increased with online voting, so this threat must be addressed by the solution design and/or processes.
Tampering with electronic records	Printed ballot papers can potentially provide evidence of tampering if this was to occur. This is not true of electronic records unless specific controls, such as the use of cryptographic signing or block chains, are put in place to do so.
Loss of the electronic ballot box	In a postal election there is a paper record of all votes received which can be used to reconstruct the election data if it is lost due to a system failure. No such record automatically exists for online votes so the solution must provide other means to ensure that the electronic ballot box is protected from loss or data corruption.
Failure or Unavailability of the Online Voting Service	There may be little discernible difference in the public mind between an online voting service being unavailable for any reason and failure of the voting systems themselves. Any disruption of online voting could be perceived as failure of the online voting solution and give cause for doubt in the integrity of an election.
Election results or process disputed	There is no New Zealand history of online voting in public elections and the electorate will be unfamiliar with the process. This may increase the likelihood that the electoral processes or election results are disputed. It is important that the chosen solution has the necessary procedural and technical controls to ensure that the results can be independently verified if they are disputed.

Table 1 High level threat categories

Threat Descriptions

Interception of Voting Papers	
Categories	Interception, vote manipulation
Description	<p>Both online and postal voting system are vulnerable to interference by a person who intercepts the voting papers addressed to another person. This is most likely to occur on an individual basis, by a person known to the victim.</p> <p>The threat profile is not materially affected by the introduction of online voting so no specific remediation is recommended.</p>
Compromised end-user device	
Categories	Interception, vote manipulation, coercion
Description	<p>The device or network that a voter uses to cast their vote online could be infected with malware that exposes an elector's vote, or allows the attacker to manipulate the vote without the elector's knowledge. It is common for this type of malware to be used for banking fraud. Common capabilities of malware include:</p> <ul style="list-style-type: none"> • Logging of keystrokes typed by the victim. • Taking snapshots of the victim's display as they interact with the computer. • Identifying and logging certain types of valuable information such as credit card details, login usernames and passwords, or other personal information. • Allowing the attacker to take control of the victim's computer, potentially without the knowledge of the victim. • Taking photographs or movies using the victim's webcam, potentially for later use for coercing the victim.
Interception of data transmitted across networks	
Categories	Interception, vote manipulation
Description	<p>Just as with a postal ballot, information sent to, and submitted by, an elector while voting online will traverse networks that may not be trustworthy and that may be outside the control of either the elector or the electoral officer. Data in transit between the online voting system and an elector's computer could be intercepted, inspected or tampered with by any party with access to any intermediate network.</p>
Compromised servers	
Categories	Interception, tampering, loss of ballot box, failure or unavailability, results disputed
Description	<p>There is a possibility that a malicious party could gain access to, or control of, components that provide the online voting service itself. This might give them the ability to breach the secrecy of the vote, disrupt voting or manipulate results, and has the potential to invalidate the election.</p>

Mass brute-force of elector credentials	
Categories	Vote manipulation, unavailability of voting system
Description	<p>An attacker attempts to guess valid elector login details in order to cast votes as those electors. The attacker does not target any specific elector, instead running through all possible combinations of login details hoping to find some that allow access.</p> <p>In some cases the high volume of connection attempts could impact the performance or availability of the online voting solution, as occurred during the Australian 2016 census.</p>
Denial of Service	
Categories	Unavailability of voting system, results disputed
Description	<p>A Denial of Service (DoS) is a common type of attack against online systems with the intention of disrupting access to system for legitimate users. This can result in the service becoming slow, unreliable or completely inaccessible. It is possible that votes submitted during an attack do not reach the online voting service, and such an event can be seen as a loss of integrity in the service, and may be reported or perceived as "hacking."</p> <p>There are three basic types of DoS attack:</p> <ul style="list-style-type: none"> • Volume based attacks; where a large amount of traffic is sent to the victim service, overwhelming the network or infrastructure to the point that it becomes inaccessible. • Protocol attacks; where a flaw or vulnerability a network protocol is used to cause equipment to exhaust its resources or crash. • Application attacks; where a flaw or vulnerability in the online software is used to cause that application exhaust its resources or crash. <p>When the attack comes from a large number of sources simultaneously it is known as a Distributed Denial of Service (DDoS). This can be from a co-ordinated group of attackers, or a "botnet" of hacked systems under the control of one or more attackers, as with the now infamous Mirai botnet.</p>

Released under the Official Information Act 1982

Service, System or Network failure Integrity of Electronic Ballot Box is Compromised	
Categories	Loss of electronic ballot box, voting service unavailable, results disputed
Description	<p>With postal voting failures of the postal system may affect some groups of electors but are unlikely to cause widespread inconvenience or disadvantage. For example, if a natural disaster interrupts postal services, the deadline for receipt of votes can be extended. If the web interface of the online voting system is to become inaccessible for any reason during the final few hours of an election this is likely to have widespread and highly visible impact.</p> <p>A problem with the networks that connect the elector to the online voting service could make the service inaccessible with similar impacts to a Denial of Service. Failure of any of the technical components that make up the online voting service could lead to the service being unreliable or inaccessible. It is possible that submitted votes could be lost, individually or en masse if the electronic ballot box is lost.</p>

Table 2 Threat descriptions mapped to threat categories

High level Security Requirements

This section describes at a high-level the attributes and security requirements necessary for the solution to meet the key objectives for the trial.

Objective	Attributes
Public Confidence	Secret, Secure, Accurate, Reliable, Recoverable, Verifiable, Access Controlled
Accessibility	Accessible, Usable
Accuracy	Accurate, Verified, Audited

Table 3 Mapping of trial objectives to solution attributes

As it is proposed to procure a solution as a service from an online voting provider these objectives are described in a way that would not limit the technical options solution provider might use to meet these objectives.

Attribute	Requirement
Secret	<ul style="list-style-type: none"> The solution MUST separately store the elector database from the electronic ballot box in such a way as to prevent any person to associate any vote with the person who cast that vote, or vice versa. <p>NOTE: There is a functional requirement that approved Electoral Officers must be able to identify the ballot paper for an elector e.g. where multiple voting occurs, or when an elector requests confirmation of their vote.</p>

Attribute	Requirement
Accurate	<ul style="list-style-type: none"> The solution MUST ensure that the vote cast accurately reflects in the intention of the voter. Note that the requirement for equivalence allows the voter to submit blank or informal votes where that is their intention. The solution MUST ensure that the vote recorded is the same as the vote cast.
Reliable	<ul style="list-style-type: none"> The solution SHOULD operate without errors and produce results that are consistent across multiple runs with the same input data. The solution MUST have the ability to continue functioning correctly and to specification even if an error has been encountered.
Accessible	<ul style="list-style-type: none"> The online voting solution MUST conform to the New Zealand Web Accessibility Standard and Web Usability Standard⁶ or another equivalent standard. The online voting solution SHOULD conform to the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0⁷
Usable	<ul style="list-style-type: none"> The solution MUST be easy to understand and use without technical expertise or training. Security controls implemented in the solution MUST NOT negatively impact the usability of the solution.
Access Controlled	<ul style="list-style-type: none"> Access to all administrative and maintenance functions in the solution MUST require user authentication using a credential unique to each individual. Access to administrative and maintenance functions MUST NOT be possible from public networks such as the Internet. Access to the voting component MUST require the elector to log in with an identifier unique to that elector, and some additional evidence, such as date of birth, to verify their asserted claim to that identifier.

⁶ <https://www.ict.govt.nz/guidance-and-resources/standards-compliance/web-standards/>

⁷ <https://www.w3.org/TR/2008/REC-WCAG20-20081211/>

Attribute	Requirement
Secure	<ul style="list-style-type: none"> • The online voting solution MUST conform to or comply with relevant New Zealand security standards, including: <ul style="list-style-type: none"> ◦ New Zealand Information Security Manual (NZISM) ◦ Protective Security Requirements (PSR) • The online voting system SHOULD be certified to an internationally agreed information security standard such as ISO/IEC 27001 or another similar standard. • The solution MUST be developed using secure software development and coding practices. • The solution MUST include incident detection and prevention capability. • The solution provider MUST maintain documented incident response plans that are communicated and regularly exercised. • The solution MUST use appropriate cryptographic signing and encryption to ensure the integrity and secrecy of the vote, such as: <ul style="list-style-type: none"> ◦ Cryptographic signing and encryption of the message payload. ◦ Cryptographic signing and encryption of the connection itself.
Available	<ul style="list-style-type: none"> • The solution MUST have sufficient capacity to meet foreseeable demand without loss of performance or availability. • The solution MUST be protected from volume based Denial of Service attacks. • The solution MUST be protected from protocols and application level denial of service attacks. • The solution architecture SHOULD allow for on-demand scalability of service capacity. • The solution SHOULD limit access from proxies or anonymisers.
Recoverable	<ul style="list-style-type: none"> • It MUST be possible in the case of system failure to recover the system to normal operation within timeframes specified in SLAs defined by the local authorities using the service. See Appendix B for a suggested method for documenting SLAs. • Recovery procedures MUST be documented and regularly exercised.
Auditable	<ul style="list-style-type: none"> • An audit log MUST be kept separately from the electronic ballot box that can be used to validate the electronic ballot box. • Audit logs MUST be proof from tampering or deletion. • It MUST be possible for the electronic ballot box to be audited if required in order to recount or resolve disputed results.
Audited	<ul style="list-style-type: none"> • The solution MUST be independently audited prior to provide assurance that the solution is secure and meets the requirements. • The solution provider SHOULD provide evidence that the solution and operation of the solution have been tested and proven to meet appropriate standards for secure operation, such as an ISAE 3402 Type 2 audit report, or an equivalent independent audit report.

Attribute	Requirement
Verifiable	<ul style="list-style-type: none"> • The solution and its protective services MUST be tested and verified as functioning correctly before the service is opened for voting. • It MUST be possible to verify that the electronic ballot box contains a complete and accurate record of the votes cast with sufficient certainty to withstand judicial review. • It MUST be possible to verify the electronic ballot box has not been altered or tampered with at any stage from the first vote cast until the records are destroyed once retention period required by the Local Electoral Act has expired. • It MUST be possible to independently verify the correct function of the voting systems, and that the correct procedures have been followed prior to, during, and after an election.

Table 4 High Level Security Requirements

Released under the Official Information Act 1982

Appendix A Conceptual model

The illustrative model below has been used for the purposes of assessing the likely security and integration requirements of any potential solution. It is not intended as a prescriptive solution architecture, and we do not expect that the eventual solution will necessarily resemble this conceptual diagram.

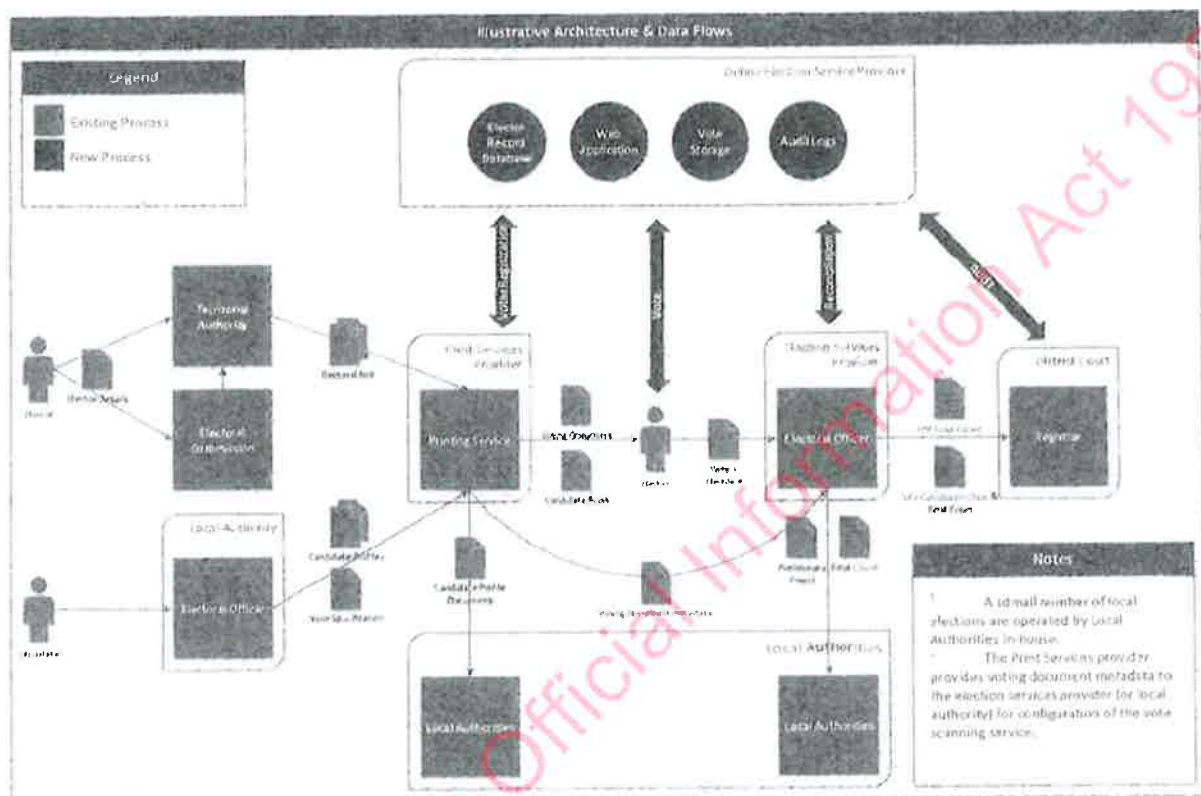


Figure 1 Illustrative solution architecture

Released under the Official Information Act 1982

Appendix B Service Levels and Availability

During an election period the required service levels and availability will vary depending on what point we are in the election cycle, especially as legislated dates draw near. The table below is suggested as a template for specifying these changing service level and availability requirements.

Date	Milestone	Service	SLA
1 July	Electoral Commission enrolment campaign starts.	Web Application	?
		Audit Logs	?
19 July	Rolls open for inspection at council offices and other sites locally. Nominations open for candidates.		n/a
16 Aug 12 p.m.	Rolls close. Nominations close 12 noon.		n/a
21 Aug	Election date and candidates' names publicised by electoral officers.		n/a
20 Sept	Voting documents begin delivery to households. Postal and Online voting open.		?
25 Sept	Voting documents complete delivery to households.		?
8 Oct	High demand period for online voting anticipated		?
12 Oct	Polling day		?
12 Oct 12:00 p.m.	Postal voting document receipt closes. New online voting sessions closes.		?
12 Oct 12:05 p.m.	In-progress online voting sessions close at 12:05 p.m.		?
12 Oct	Preliminary vote counts sent to Electoral Office		?
12 Oct	Preliminary results announced		?
17-23 Oct	Official results (including all valid ordinary and special votes) declared.		?
	Voting and electoral documents lodged with Registrar of District Court		?
+ 6 Months	Voting and electoral documents Destroyed		n/a

Table 5 Example service level specification table

1.

Appendix C Past Recommendations

These high-level security recommendations are quoted from the 2014 Report from the Online Voting Working Party.⁸ These recommendations are upheld for the proposed 2019 trial with some changes as described in this document.

Recommendation Five

The [project] and its strategic partners should involve security experts throughout the process, including at the very early specification and design stages, to ensure that online voting systems are appropriately secure.

Recommendation Six

The [project] should undertake a detailed threat analysis to inform security decisions made as a part of protecting online voting systems.

Recommendation Seven

In order to ensure that online voting systems are secure enough, the [project] should harness the expertise of the wider security community through a 'bug bounty' or similar process to attract constructive analysis of proposed systems for vulnerabilities.

Recommendation Eight

The [project] should ensure that any online voting solutions are highly auditable.

Recommendation Eleven

Testing and non-politically binding trials should be undertaken prior to the 2016 local elections to ensure that online voting systems are ready for use in a political contest.

Recommendation Thirteen

The [project] should ensure that any findings, audits, and reviews in relation to the delivery of online voting are publicly available in an appropriate form to foster understanding and trust in the transparency and rigour of the delivery process.

Recommendation Eighteen

For the 2016 trials, online voting should:

- a. use the existing postal ballot issue to communicate login details to users
- b. only allow one-time access to the online voting system

⁸ [https://www.dia.govt.nz/vwluResources/Online-Voting-in-New-Zealand-Report-of-the-Online-Voting-Working-Party-pdf/\\$file/Online-Voting-in-New-Zealand-Report-of-the-Online-Voting-Working-Party-pdf.pdf](https://www.dia.govt.nz/vwluResources/Online-Voting-in-New-Zealand-Report-of-the-Online-Voting-Working-Party-pdf/$file/Online-Voting-in-New-Zealand-Report-of-the-Online-Voting-Working-Party-pdf.pdf)

Appendix D References

Online Voting in New Zealand: Feasibility and options for local elections,
[https://www.dia.govt.nz/vwluResources/Online-Voting-in-New-Zealand-Report-of-the-Online-Voting-Working-Party-pdf/\\$file/Online-Voting-in-New-Zealand-Report-of-the-Online-Voting-Working-Party-pdf.pdf](https://www.dia.govt.nz/vwluResources/Online-Voting-in-New-Zealand-Report-of-the-Online-Voting-Working-Party-pdf/$file/Online-Voting-in-New-Zealand-Report-of-the-Online-Voting-Working-Party-pdf.pdf)

Requirements for a trial of online voting in local elections,
[https://www.dia.govt.nz/vwluResources/Reqs-for-trial-online-voting-in-local-elections-Nov15-docx/\\$file/Reqs-for-trial-online-voting-in-local-elections-Nov15-docx.docx](https://www.dia.govt.nz/vwluResources/Reqs-for-trial-online-voting-in-local-elections-Nov15-docx/$file/Reqs-for-trial-online-voting-in-local-elections-Nov15-docx.docx)

Online voting for local elections – Early market engagement report v0.1, Adam Stapleton 2014,
<https://dia.cohesion.net.nz/Sites/GCIO/AOGA/ReferenceLibrary/Online%20voting%20-%20Early%20market%20engagement%20report%20v0.1.pdf?Web=1>

Security Analysis of the Estonian Internet Voting System,
<https://jhalderm.com/pub/papers/ivoting-ccs14.pdf>

Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, Council of Europe 2017,
https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f#_ftn1

Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, Council of Europe 2017,
https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168071bc84

Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting, Council of Europe,
https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726c0b

Observation of e-enabled elections, Presentation to Council of Europe Workshop, Jonathan Stonestreet 2010,
https://www.coe.int/t/dgap/goodgovernance/Source/EVoting/Workshops/Transparency/Oslo_18-19March/Stonestreet.ppt

Observing E-enabled Elections: How to Implement Regional Electoral Standards, Jordi Barrat, International Institute for Democracy and Electoral Assistance 2012,
<https://www.idea.int/publications/catalogue/observing-e-enabled-elections-how-implement-regional-electoral-standards>

From: 9(2)(a);(a)
Sent: Monday, 13 August 2018 5:28 PM
To: 9(2)(a)
Cc: 9(2)(a); 9(2)(a); 9(2)(a); 9(2)(a); 9(2)(a); 9(2)(a)
Subject: Feedback for Online Voting Trial Key Requirements, Auckland Council

Hi 9(2)(a)

My feedback is below.

Regards,
9(2)(a)

General suggestions

1. Wherever possible keep requirements focussed on **outcomes** (what we want to achieve) rather than outputs (how we want to achieve it). This gives the respondents room to suggest their best approach to meeting expectations.
2. This re opens the decision for **pre-registration** or not. I think that it will be important to work through the benefits and issues regarding pre-registration; what threats and risks is it intended to mitigate?
3. Document **required outcomes for the trial** as well as the online voting system, e.g.
 - a. What do they want to learn from the trial?
 - b. How will the trial solution contribute to, or provide the basis for, a production online voting solution?
 - c. What value can the trial provide for better understanding and preparation for potential future parliamentary elections?
 - d. How will a go/no go decision be made for the 2019 local body elections?
 - e. What is "plan b" if the 2019 local election target cannot be met (e.g. trial for the next by election?)

Specific feedback on system requirements

FR-007	Appears to combine 3 separate requirement statements. Some ambiguity in wording ("election" vs "issue"). Presupposes a solution ("warning message") rather than an outcome.
FR 008	Appears to combine 2 separate requirement statements. Narrative in comment ("prevent screenshots") may be impossible to enforce.
NFR 008	Presupposes a solution rather than expressing a desired outcome. See suggestion 2. above re: pre registration.
NFR-011	Contradicts NFR-005 (allowing blank or informal votes)
NFR 015	I suggest including an SLA specification as an appendix to the requirements document and referring to it here. See the suggested SLA matrix in <i>Modernising Voting Draft Security Recommendations</i> , Appendix B Service Levels and Availability.
NFR-017	This reads as though there is an expectation for electors to use multiple factor authentication to access the voting application. This is unlikely to be workable in practice. Note that an identifier (username, id number etc) is not an authentication factor. The requirement incorrectly lists <i>Modernising Voting Draft Security Recommendations</i> as a source.
NFR-018	Appears to combine two separate requirements.

NFR-020	The feasibility of this requirement should be tested with prospective respondents before issuing the RFP, and perhaps this should be a SHOULD rather than MUST requirement. One of the two New Zealand election services providers has expressed a strong preference not to take this approach.
NFR-022	The SLA targets described in this requirement are superficial and unlikely to deliver the intended outcome. See the suggested SLA matrix in <i>Modernising Voting - Draft Security Recommendations, Appendix B Service Levels and Availability</i> .
NFR-026	As written this may result in the online voting application becoming inaccessible to the majority of electors. Most Internet users are likely to be accessing the application through ISP or business proxies.
NFR-026	Wording is unclear. Appears to include 2 separate requirements.
NFR-028	Meaning is unclear
NFR-035	Meaning is unclear and doesn't reflect the intention of the source. Usually better worded as something like "please describe your conformance or compliance with New Zealand and international security standards, and how each of these standards is applied in the governance, management, development and operation of your proposed solution."
NFR-041	Meaning is unclear.
NFR-049	Meaning is unclear

From: 9(2)(a)
Sent: Monday, 13 August 2018 10:50 AM
To: 9(2)(a) 9(2)(a)(2)(a) 9(2)(a) 9(2)(a)2(a) 9(2)(a) 9(2)(a)
Cc: 9(2)(a) 9(2)(a)2(a)
Subject: On-line voting requirements

Hi all

Following on from our meeting last week did anyone have any feedback on the requirements that we were provided, I have heard from [redacted] but no one else yet (unless I've missed your emails, in which case I apologise).

Can I have a response today please.

Cheers

9(2)(a) | 9(2)(a) | 9(2)(a)
The Department of Internal Affairs Te Tari Taiwhenua
 Direct Dial: + 9(2)(a) 2(a)
 9(2)(a) 45 Pipitea Street, PO Box 805, Wellington 6140, New Zealand



Te Tari Taiwhenua
Internal Affairs

From: 9(2)(a)) (a)
Sent: Thursday, 4 October 2018 4:32 PM
To: 9(2)(a) 9(2)(a) 9(2)(a)
Cc: 9(2)(a)
Subject: RE: Security and disposal of records discussion

Link to draft recommendations as discussed.

<https://dia.cohesion.net.nz/Sites/GCIO/AOGA/ layouts/15/DocIdRedir.aspx?ID=4UAZY7VS6QRJ-101908526 28>

-- 9(2)(a)

-----Original Appointment-----

From: 9(2)(a)
Sent: Thursday, 4 October 2018 1:04 PM
To: 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)) (a)
Cc: 9(2)(a)
Subject: Security and disposal of records discussion
When: Thursday, 4 October 2018 3:30 PM-4:00 PM (UTC+12:00) Auckland, Wellington.
Where: 9(2)(a)

Released under the Official Information Act 1982

Kate MacDonald

From: 9(2)(a)
Sent: Tuesday, 17 July 2018 3:42 PM
To: 9(2)(a)
Cc: 9(2)(a)
Subject: RE: Draft Cabinet paper for departmental comment online voting trials
Attachments: Online voting trial cabinet paper - AJS Notes.docx

I attach a copy of the draft paper marked up with a small number of tracked changes and comments.

9(2)(a)

From: 9(2)(a)
Sent: Tuesday, 17 July 2018 12:45 PM
To: 9(2)(a)
Subject: RE: Draft Cabinet paper for departmental comment - online voting trials

Hi 9(2)(a)

Please send direct to 9(2)(a) and 9(2)(a) cc 9(2)(a) and me.

Cheers

9(2)(a)

From: 9(2)(a)
Sent: Tuesday, 17 July 2018 9:25 AM
To: 9(2)(a)
Subject: RE: Draft Cabinet paper for departmental comment - online voting trials

Should I be sending my feedback on the cabinet paper to you? I see we have to get our comments back by c.o.p (close of parliament?) today.

9(2)(a)

From: 9(2)(a)
Sent: Monday, 16 July 2018 11:28 AM
To: 9(2)(a)
Subject: FW: Draft Cabinet paper for departmental comment - online voting trials

With 9(2)(a) response ...

From: 9(2)(a)
Sent: Monday, 16 July 2018 11:24 AM
To: 9(2)(a)
Subject: FW: Draft Cabinet paper for departmental comment - online voting trials

FYI

From: 9(2)(a)
Sent: Friday, 13 July 2018 3:27 PM
To: 9(2)(a)
Cc: 9(2)(a)
Subject: RE: Draft Cabinet paper for departmental comment - online voting trials

I think the paper is good, with one exception discussed below. I've made a few comments and suggested a few changes in the attached. Note that the comments on para 36 re GCDO engagement should be checked by other SLT members before our feedback is submitted.

The exception is that I don't think the particular security risks associated with online voting are highlighted sufficiently. In para 30, the risk of vote manipulation is even downplayed by referring to the risk as "perceived", while all the other risks listed are referred to as "potential". At minimum, this should be brought into alignment with the others.

Also I can't help being aware that there is a strong body of thought that argues on line voting can never be made secure to mass manipulation and that current efforts fall well short of acceptable. A google search will show recent articles from reputable sources that strongly criticise the security of many online elections, including those run in NSW in 2015 and even in Estonia, who have been doing it the longest. I'm not an expert and can't say if these concerns are overblown, but it seems prudent at least to acknowledge there is considerable controversy as a reason to pay the utmost attention to issues of architecture, testing and other aspects of security in any trial. I think this is an important point for GCDO to make, as issues of integrity are the most likely to draw our Minister into any fallout associated with a problematic online trial.

The paper could also include an expectation that efforts be made to understand lessons learned in other jurisdictions, though this could also be left for the more detailed GCDO advice that will follow.

I haven't included any of this in my comments attached (except for changing perceived to potential), as I wanted to raise the concern with this group first. I'm happy to craft such feedback if people agree we should be stronger on this point.

9(2)(a)

From: 9(2)(a) 9(2)(a)
Sent: Friday, 13 July 2018 9:44 AM
To: 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
9(2)(a) 9(2)(a) 9(2)(a)
Cc: 9(2)(a) 9(2)(a)
Subject: RE: Draft Cabinet paper for departmental comment - online voting trials

Please note that we've agreed to review this based on GCDO providing a similar level of oversight to this local authority initiative as we would to a high profile public service one. This is on the basis that:

- Cabinet will likely expect Minister Curran to be able to comment on this
- Any solution needs to be safe, secure and extensible at least across the local authorities (not just the initial club) and ideally for general elections in the future
- GCDO will be expected to provide investment advice, as well as assurance oversight, privacy, commercials potentially et al
- It's an opportunity, potentially, for Ministers Curran and Mahuta to jointly announce something

In other words, we'll just need to find a way to engage on this irrespective of the fact that it's outside current mandate funding, resourcing...

Our advice should be to help ensure that the Cab paper/ policy is not limiting or short sighted, and aligns to the digital strategy/ agenda.

Thanks, 9(2)(a)

From: 9(2)(a) 9(2)(a)
Sent: Friday, 13 July 2018 9:31 AM
To: 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
Cc: 9(2)(a) 9(2)(a)
Subject: FW: Draft Cabinet paper for departmental comment - online voting trials

Hi 9(2)(a)

Attached is a copy of the draft Cabinet paper for online voting trials for Department feedback. Please let me know if you have any feedback.

I've asked the team working on this item to include an update in the status report for next week.

Thanks

9(2)(a)

From: 9(2)(a)
Sent: Thursday, 12 July 2018 3:43 PM
To: 9(2)(a); 9(2)(a)
Cc: 9(2)(a)
Subject: FW: Draft Cabinet paper for departmental comment - online voting trials

Hi 9(2)(a)

See the attached for the Cabinet paper I mentioned last Friday (I didn't forget!). Is there anyone else within SST that I should forward this to? We're working to an even tighter timeframe than originally intended so we're now looking for comment by close of play next Tuesday. My apologies for the short turnaround.

Cheers,

From: 9(2)(a)
Sent: Thursday, 12 July 2018 12:21 PM
To: 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
Cc: 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
Subject: Draft Cabinet paper for departmental comment - online voting trials

Kia ora koutou

As previously mentioned please find attached the draft Cabinet paper, re proposed online voting trials, for your comment.

Apologies for the short turnaround but can you please any comments back by c.o.p. **Tuesday 17 July**. As I will be out of the office on Monday and Tuesday can you please send the responses to 9(2)(a) (9(2)(a) copied to me. That would be much appreciated.

If you wish to discuss any of the contents or context for the Cabinet paper by phone please contact:

Friday: 9(2)(a) 9(2)(a) 9(2)(a)
Monday or Tuesday: 9(2)(a) 9(2)(a) 9(2)(a)

At this stage our proposed timeline is for CBC to consider this paper on Monday 20 August.

9(2)(a) | 9(2)(a) | 9(2)(a)
The Department of Internal Affairs Te Tari Taiwhenua
Direct Dial: 9(2)(a) PO Box 805, Wellington 6140, New Zealand |
www.dia.govt.nz

From: 9(2)(a)
Sent: Tuesday, 24 October 2017 4:51 PM
To: 9(2)(a); 9(2)(a)
Subject: FW: Modernising voting - Expertise on

Hi 9(2)(a)

See below for your comment please. I suggest you go wider than 2.53-2.56, and perhaps review the EU / Council of Europe precursor documents at:
<https://www.coe.int/en/web/electoral-assistance/e-voting>

Overall my comment is that requirements should be:

- Meaningful
- Quantified where possible
- Achievable
- Consistent

Not sure if the current document (2015 Requirements) meets these. Feel free to comment frankly.

Cheers

9(2)(a)

From: 9(2)(a)
Sent: Tuesday, 24 October 2017 2:01 p.m.
To: 9(2)(a)
Cc: 9(2)(a)
Subject: Modernising voting - Expertise on

Hi 9(2)(a)

Can I please check with you on the best point of contact for some advice on security and assurance service level targets for the online voting trial in local elections?

We are working with the local government sector representatives to review the 2015 Requirements to check that they are still fit for purpose. The intention is that some of these requirements will be the basis for regulations for online voting trials, and that others will be part of the Service Level Agreement that councils will have with the online service provider

The sector has asked us to seek SST/GCIO input on the following:

- advice on whether the security requirements (Requirements 2.53 – 2.56) are still up to date and reflect best practice
- whether Requirement 2.22 (which prevents vote and voter information being transmitted or held outside NZ) is still required or whether the cloud-related Requirements (2.59 and 2.60) are sufficient
- attending the next Expectations working group meeting. [LGNZ and SOLGM are inviting representatives from InternetNZ and the Association of Local Government Information Management (ALGIM) to attend the meeting to discuss security and assurance and they are keen to have someone from DIA with expertise in this area attend also. The workshop is on Wednesday 1 November from 11-3pm. I would anticipate that this agenda item could be 1.5 2hrs but SOLGM have said they are happy to be flexible about where on the agenda this item is to help work around diaries.]

On the issue of information being held overseas, 9(2)(a) has put us in touch with 9(2)(a) and we're going to catch up with him about that.

On the other matters are you the best point of contact?

Thanks,
9(2)(a)

9(2)(a) | 9(2)(a) | 9(2)(a)
The Department of Internal Affairs Te Tari Taiwhenua
Direct Dial: 9(2)(a) 9(2)(a)

Released under the Official Information Act 1982

9(2)(a)

From: 9(2)(a):(a)
Sent: Tuesday, 17 July 2018 3:42 PM
To: 9(2)(a):(a) 9(2)(a):(a)
Cc: 9(2)(a) 9(2)(a)
Subject: RE: Draft Cabinet paper for departmental comment - online voting trials
Attachments: Online voting trial cabinet paper - AJS Notes.docx

I attach a copy of the draft paper marked up with a small number of tracked changes and comments.

-- 9(2)(a)

From: 9(2)(a)
Sent: Tuesday, 17 July 2018 12:45 PM
To: 9(2)(a):(a)
Subject: RE: Draft Cabinet paper for departmental comment - online voting trials

Hi 9(2)(a)

Please send direct to 9(2)(a) and 9(2)(a) cc 9(2)(a) and me.

Cheers

9(2)(a)

From: 9(2)(a):(a)
Sent: Tuesday, 17 July 2018 9:25 AM
To: 9(2)(a)
Subject: RE: Draft Cabinet paper for departmental comment - online voting trials

Should I be sending my feedback on the cabinet paper to you? I see we have to get our comments back by c.o.p (close of parliament?) today.

-- 9(2)(a)

From: 9(2)(a)
Sent: Monday, 16 July 2018 11:28 AM
To: 9(2)(a):(a)
Subject: FW: Draft Cabinet paper for departmental comment - online voting trials

With 9(2)(a) response ...

From: 9(2)(a)
Sent: Monday, 16 July 2018 11:24 AM
To: 9(2)(a)
Subject: FW: Draft Cabinet paper for departmental comment - online voting trials

FYI

From: 9(2)(a)
Sent: Friday, 13 July 2018 3:27 PM
To: 9(2)(a) 9(2)(a) 9(2)(a):(a) 9(2)(a):(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
Cc: 9(2)(a) 9(2)(a)
Subject: RE: Draft Cabinet paper for departmental comment - online voting trials

I think the paper is good, with one exception discussed below. I've made a few comments and suggested a few changes in the attached. Note that the comments on para 36 re GCDO engagement should be checked by other SLT members before our feedback is submitted.

The exception is that I don't think the particular security risks associated with online voting are highlighted sufficiently. In para 30, the risk of vote manipulation is even downplayed by referring to the risk as "perceived", while all the other risks listed are referred to as "potential". At minimum, this should be brought into alignment with the others.

Also I can't help being aware that there is a strong body of thought that argues on line voting can never be made secure to mass manipulation and that current efforts fall well short of acceptable. A google search will show recent articles from reputable sources that strongly criticise the security of many online elections, including those run in NSW in 2015 and even in Estonia, who have been doing it the longest. I'm not an expert and can't say if these concerns are overblown, but it seems prudent at least to acknowledge there is considerable controversy as a reason to pay the utmost attention to issues of architecture, testing and other aspects of security in any trial. I think this is an important point for GCDO to make, as issues of integrity are the most likely to draw our Minister into any fallout associated with a problematic online trial.

The paper could also include an expectation that efforts be made to understand lessons learned in other jurisdictions, though this could also be left for the more detailed GCDO advice that will follow.

I haven't included any of this in my comments attached (except for changing perceived to potential), as I wanted to raise the concern with this group first. I'm happy to craft such feedback if people agree we should be stronger on this point.

9(2)(a)

From: 9(2)(a) 9(2)(a)
Sent: Friday, 13 July 2018 9:44 AM
To: 9(2)(a)2(a) 9(2)(a)(a) 9(2)(a)2(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)(2)(a) 9(2)(a)
9(2)(a) 9(2)(a) 9(2)(a)
Cc: 9(2)(a) 9(2)(a)
Subject: RE: Draft Cabinet paper for departmental comment - online voting trials

Please note that we've agreed to review this based on GCDO providing a similar level of oversight to this local authority initiative as we would to a high profile public service one. This is on the basis that:

- Cabinet will likely expect Minister Curran to be able to comment on this
- Any solution needs to be safe, secure and extensible at least across the local authorities (not just the initial club) and ideally for general elections in the future
- GCDO will be expected to provide investment advice, as well as assurance oversight, privacy, commercials potentially, et al
- It's an opportunity, potentially, for Ministers Curran and Mahuta to jointly announce something

In other words we'll just need to find a way to engage on this irrespective of the fact that it's outside current mandate, funding, resourcing...

Our advice should be to help ensure that the Cab paper/ policy is not limiting or short sighted, and aligns to the digital strategy/ agenda.

Thanks, 9(2)(a)

From: 9(2)(a)(a)
Sent: Friday, 13 July 2018 9:31 AM
To: 9(2)(a)(a) 9(2)(a)2(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)(2)(a) 9(2)(a) 9(2)(a)
9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
Cc: 9(2)(a) 9(2)(a)
Subject: FW: Draft Cabinet paper for departmental comment - online voting trials

Hi 9(2)(a)

Attached is a copy of the draft Cabinet paper for online voting trials for Department feedback. Please let me know if you have any feedback.

I've asked the team working on this item to include an update in the status report for next week.

Thanks

9(2)(a)

From: 9(2)(a)
Sent: Thursday, 12 July 2018 3:43 PM
To: 9(2)(a)
Cc: 9(2)(a)
Subject: FW: Draft Cabinet paper for departmental comment - online voting trials

Hi 9(2)(a)

See the attached for the Cabinet paper I mentioned last Friday (I didn't forget!). Is there anyone else within SST that I should forward this to? We're working to an even tighter timeframe than originally intended so we're now looking for comment by close of play next Tuesday. My apologies for the short turnaround.

Cheers,

From: 9(2)(a)
Sent: Thursday, 12 July 2018 12:21 PM
To: 9(2)(a)
Cc: 9(2)(a)
Subject: Draft Cabinet paper for departmental comment - online voting trials

Kia ora koutou

As previously mentioned please find attached the draft Cabinet paper, re proposed online voting trials, for your comment.

Apologies for the short turnaround but can you please any comments back by **c.o.p. Tuesday 17 July**. As I will be out of the office on Monday and Tuesday can you please send the responses to 9(2)(a) 9(2)(a) copied to me. That would be much appreciated.

If you wish to discuss any of the contents or context for the Cabinet paper by phone please contact:

Friday: 9(2)(a)

Monday or Tuesday: 9(2)(a)

At this stage our proposed timeline is for CBC to consider this paper on Monday 20 August.

9(2)(a)

The Department of Internal Affairs Te Tari Taiwhenua

Direct Dial: 9(2)(a)

www.dia.govt.nz

PO Box 805, Wellington 6140, New Zealand |

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

Office of the Minister of Local Government

Chair
Cabinet Economic Development Committee

A regulatory approach to enable local government online voting trials in 2019

Proposal

1. This paper seeks agreement to a regulatory approach to enable limited online voting trials in the 2019 local authority elections.
2. The preferred approach proposes the regulations specify the high-level performance requirements and outcomes for online voting. Responsibility for compliance with those regulations, including ensuring the security and integrity of the election, would lie with local authorities.
3. To minimise risks, the regulations will specify that only a subset of councils (members of a planned working group to design and procure an online voting solution) may undertake a trial.

Commented [KS1]: And that the same platform will be used by all?

Executive summary

4. <insert text>

Background

Without a regulatory framework for online voting electoral processes will become increasingly out of step with public expectations and needs

5. Under the Local Electoral Act 2001 (the Local Electoral Act) and the Local Electoral Regulations 2001 (the Local Electoral Regulations), local authorities are responsible for conducting local elections and polls in their districts, including elections to regional councils, district health boards (DHB's), local boards, community boards and licensing trusts.
6. Central government is responsible for maintaining the regulatory framework for local elections. This involves ensuring that the framework maintains the integrity of local electoral systems and democracy and that there is public acceptance of the legitimate mandates of elected councils.
7. Regulations allow for local authorities to administer elections either via postal voting or booth voting. Local authorities currently rely solely on postal voting for the conduct of local body elections. Postal voting is becoming increasingly out of step with public expectations and real world practicalities.

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

8. In a 2016 post-election voter awareness survey conducted by Auckland Council, 74 per cent of respondents said they would prefer online voting to postal voting.¹ The results showed that this preference for online voting occurred across all age categories. Additionally, some groups of electors have difficulty participating in the existing postal ballot system due to reasons such as geographical distance or physical impairment (e.g. the blind may require assistance completing the vote). Online voting provides opportunities to increase accessibility for these electors.
9. Postal voting is also heavily dependent on services provided by New Zealand Post (NZ Post). NZ Post is in a process of transition as ordinary mail volumes continue to decrease and postal services are adjusted. As this transition occurs, supporting postal voting in local elections is putting an increasing strain on the postal network at those peak times.²
10. There are a range of interim options which are currently available to supplement or support the postal. However, online voting is a more enduring solution to these challenges, and one more in step with public expectations and wider Government objectives for digital transformation. Therefore, the trial of online voting at local elections is a local government sector priority.

Cabinet has agreed to enabling legislation and noted future papers on regulations to enable trials and a wider Modernising Voting work programme

11. In March 2018 Cabinet agreed to amendments to the Local Electoral Act. The amendments enable regulations to be promulgated that (amongst other things) authorise a local authority to trial a new voting method for a specified subset of electors at an election (DEV 18 Min 0022). The Local Electoral Matters Bill (the Bill), which includes the necessary amendments (and related policy decisions), has been introduced to the House of Representatives and is currently before the Justice Committee. A report back on the Bill is due on 9 November 2018, and it is intended that the amendments be enacted in December 2018 in order to facilitate a potential trial of online voting in 2019.
12. A trial of online voting is a key part of the Modernising Voting Review (the Review). The Review, signalled to Cabinet in March 2018 (DEV 18 Min 022), encompasses a programme of work to modernise local authority electoral processes and put in place a more enduring platform for voting in local elections. The objectives for the Review were developed in conjunction with the Department of Internal Affairs, the NZ Society of Local Government Managers (SOLGM), and Local Government New Zealand (LGNZ). It is intended that the review will be conducted as a partnership between these three parties.
13. At the time, I indicated my intention to report back to Cabinet with proposals for:
 - 13.1 the finalised Terms of Reference for the Review; and
 - 13.2 a trial(s) of online voting, including the content of regulations to authorise online voting trials and consideration of the financial implications of any such trial.

¹ <http://knowledgeauckland.org.nz/assets/publications/TR2017-013-Awareness-attitudes-voting-in-2016-Auckland.pdf>

² Based on current mail volumes, delivering the postal ballots represents a 30% increase in mail volume for the week when postal ballots are delivered for triennial local elections.

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

A proposed sector wide approach to an online voting trial in 2019 has been abandoned

14. Further work between the Department, LGNZ and SOLGM has concluded that the preferred approach for a 2019 trial (a national trial, coordinated by a sector collective in partnership with central government, contracting with a single provider on behalf of multiple councils) is not feasible. Such an approach would have required significant expertise and experience in collaborative IT project management which was unavailable within the required timeframe and resourcing. As a result, LGNZ and SOLGM have signalled that work on this approach has stopped.

However Auckland and some other councils remain interested in conducting a trial in 2019

15. On 24 May 2018, the Auckland Council Governing Body voted to support, in principle, an online voting trial at the 2019 local elections, subject to:
 - 15.1 the Bill and enabling regulations being passed in time to procure and implement an online voting solution;
 - 15.2 all risks, including security risks, being appropriately managed;
 - 15.3 an assessment of the cost of a trial; and
 - 15.4 final approval for any trial by the Governing Body.
16. Several other councils (Wellington City Council, Hamilton City Council, Māhorua District Council, Matamata-Plato District Council, Tararua District Council, and Selwyn District Council) have obtained in-principle support for a 2019 trial from their elected members subject to similar conditions. In-principle support is also currently being sought by Palmerston North City Council and Gisborne District Council, while Masterton District Council and Tauranga City Council are also considering the issue.
17. The proposal is that interested councils form a working party to design and procure for a trial, sharing the costs and staff resources. These "member" councils are currently collaboratively developing a memorandum of understanding to guide the conduct for organising and running the trial.

To enable 2019 trials, Cabinet commitment to the proposed regulatory approach will be required in September

18. The member councils draft timeframe for the trial relies on the content of the regulations being sufficiently well understood by the end of August to allow a request for proposal (RFP) for online voting services to be issued in September 2018. While the timeframe allows for the regulations themselves to be in place by March 2019, the RFP will need to include sufficient information about the proposed regulatory framework to allow the tender process to include realistic pricing. This will allow Councils to assess the acceptability of the costs of the trial. Therefore, any delays in the promulgation of regulations are likely to affect the ability for Councils to undertake a trial in 2019.

Implementing a regulatory framework for the trial

19. As part of taking a partnership approach with local government, I am seeking to implement a regulatory framework that will enable this trial for 2019. In order to minimise the risks associated with implementing a new regulatory framework, it is intended that the trial will be limited to member councils. Therefore the enabling regulatory framework will only apply to members of the working group.

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

20. Due to tight timeframes and costs that may prove prohibitive, there is a risk that the trial may not go ahead in 2019. The feasibility of a trial may not be known until after member councils have undertaken their RFP processes. Delaying a trial of online voting would potentially allow the Review to consider wider changes to the local electoral framework before committing to a trial. Further, delaying a trial would leave time for technical confidence and public acceptance of online voting to grow.
21. Nonetheless, I recommend proceeding with the establishment of a regulatory framework. The uncertainties around how long postal voting in its current state will be sustainable for local government places time pressure on the investigation of online voting. Furthermore, this trial is intended to be the first in a series, with the goal of undertaking more substantive trials in future elections (both interim elections and referenda and at the 2022 triennial elections).
22. If a trial proves unfeasible in 2019, my officials will continue to work with councils towards the goal of implementing online voting as soon as possible thereafter. Therefore I recommend that these regulations would apply to both the 2019 triennial elections and interim by-elections and referenda prior to the 2022 election.

Proposal: a high level enabling framework that places responsibility for the integrity and security of elections on local authorities

23. I propose that an enabling regulatory framework similar to that for other current voting methods be established. Under this approach, Government prescribes the procedures, safeguards and outcomes that the operation of a voting method must achieve. The legal responsibility for complying with the regulatory framework and ensuring the integrity and security of elections is the responsibility of the local authority electoral officers and their staff.
24. The member councils would be responsible for:
- 24.1 project management, timeline and milestones;
 - 24.2 risk management;
 - 24.3 security, authentication and verifiability design and testing;
 - 24.4 vendor selection approach and contracting;
 - 24.5 communications and engagement; and
 - 24.6 implementation.
25. This approach would be similar to that which currently exists for postal voting. Under regulations, electoral officers would have responsibility for posting voting documents to the residential or postal addresses of electors as under the status quo. However, the postal documents could provide electors with the choice to either vote by post or via the Internet, and would include instructions and an authentication code for voting online.

Commented [A352]: What does this refer to? Recommendation was to use the existing elector number (generated randomly and printed on papers by NZ Post) and the elector DOB

Maybe? Elector # + code?
Code + drb?
What?

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

Alternative approaches to the regulatory framework are not practical given current timeframes

26. Another approach to an online voting trial would be to implement a regulatory framework similar to that considered by the previous Government for proposed trials in 2016. Under that approach, councils wishing to participate in trials were required to demonstrate to Government that their systems would meet an extensive list of technical and security requirements (developed from guidance issued by the Council of Europe) before being authorised to utilise the trial voting method.
27. Given the time constraints, it would be impossible to develop the necessary set of detailed technical regulatory requirements in time for the 2019 elections. The implementation of this approach will therefore need to be delayed until triennial local elections in 2022. By this time, already existing pressures on the postal voting system will have likely intensified, creating the risk that voting system will no longer be fit for purpose or cost-viable for councils.
28. Furthermore, I consider that my proposal – where the incentives for delivery lie with the sector within an outcomes-based framework – is most consistent with a partnership approach between central and local government where the parties engage each other with mutual respect and understanding.

There are problems and risks with online voting that necessitate different regulatory requirements from those for postal voting

29. There are inherent risks within the current postal system including:
 - 29.1 the loss or theft of voting papers;
 - 29.2 being non-verifiable as while the voter may find out if a vote was recorded under their name, they have no way of knowing if their ballot was recorded as cast;
 - 29.3 inability to prevent voting papers from being intercepted and submitted fraudulently;
 - 29.4 the privacy of voting cannot be controlled, and voting may be coerced; and
 - 29.5 the nature of postal-voting means that some individuals (e.g. the blind) are incapable of voting independently.
30. The public has a high degree of tolerance for these risks due to trust and familiarity with the postal system and a general history of success with postal voting. However, while the general risk profiles of online voting and postal voting are similar, several risks pose additional challenges for the successful conduct of an online voting trial, including:
 - 30.1 the ~~perceived~~ potential opportunities for a malicious party to intercept or manipulate votes *en masse*;
 - 30.2 the potential for a privacy breach that results breach of personal information and voting record of a large number of voters in access to a large amount of personal information;
 - 30.3 the potential lack of a paper record of votes that could be used to reconstruct election data in the event of a system failure;
 - 30.4 the potential for the web interface to fall during the final hours of an election, thereby having a widespread and visible impact on people's ability to vote; and

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

30.5 the lack of a history of successful online voting causing lower trust and potentially increased likelihood of a vote being challenged and/or a recount demanded.

31. If an online voting trial were to suffer significant failure – either as a result of a technical malfunction or due to malicious activity – this could significantly damage public trust in online voting, potentially delaying future attempts to introduce online voting for local elections and other democratic processes such as general elections or referenda. Robust system design, regulatory requirements, assurance auditing, testing and implementation processes can mitigate the risks of a negative outcome. It is critically important that the trial is well planned, well-resourced and of high quality. It is therefore necessary that the regulatory framework establish a number of high-level outcomes and requirements to minimise the potential for failure.

Identifying and managing risks to achieve desired outcomes

32. My officials are working closely with the member councils. I am confident that councils clearly understand the risks and that they have given the Department reasonable assurance that risks will be effectively managed. However, central government has a strong interest in the integrity of the local election voting system and public acceptance of the legitimacy of outcomes.
33. Therefore, it is necessary that regulations require that before a trial can be conducted territorial authorities first receive a published report from their Chief Executive, advising that they are satisfied that the solution is consistent with a number of desired outcomes. These outcomes seek to address the risks signalled in paragraph 30 above, and include that the online voting solution is:
- 33.1 secret, so that data is stored in a way that prevents any person from being able to associate a vote to an individual without that individual's consent;
 - 33.2 accurate, so that the vote cast accurately reflects the intentions of the voter and is recorded as such;
 - 33.3 available and reliable, so that the system performs as intended and an individual can cast their vote at all times that postal voting is also available;
 - 33.4 auditable, so that the electronic ballot box can be reviewed in the event of a recount or a disputed vote;
 - 33.5 verifiable, so that it is possible to verify that the electronic ballot box contains a complete and accurate record of the votes cast; and
 - 33.6 secure so that the solution complies with relevant New Zealand and international security standards and includes documented incident response plans.
34. Given the risks inherent in a failed online voting trial, it is also necessary that the proposed online voting solution be independently audited to provide assurance that the solution is secure and meets the criteria set out above. Furthermore, given the importance of the 2019 online trial to future online voting, I recommend that the regulations restrict the ability to conduct a trial to member councils. This will help to minimise the risk, given the substantial work that the member councils are undertaking into the necessary risk assessment and planning for a trial.

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

The GCDO will engage with the member councils regarding what type of support they require.

35. In developing an online voting solution it is intended that local authorities would work together with central government, taking a partnership approach to ensuring that the outcomes set out above are met. This would include working closely with the Minister of Government Digital Services to assess how the Government Chief Digital Officer (GCDO) may assist member councils with the development of their online voting solution.
36. In particular, GCDO officials have signalled that they could provide support and guidance to councils undertaking the online voting trial. This support could include engaging with member councils to provide:
 - 36.1 advice around security architecture;
 - 36.2 guidance and a framework for project assurance;
 - 36.3 advice about potential service providers procurement of systems and services;
 - 36.4 advice regarding the potential for RealMe to serve as a mechanism for voter identification;
 - 36.5 assessments of whether the GCDO's work on the future of digital identity can potentially support the development of a viable online voting option; and
 - 36.6 input on how the GCDO's service innovation approach can support online voting.

Commented [KS3]: Right wording?

Commented [AJS4]: In order to maximise participation in the online voting it was agreed that pre-registration, as would be required by RealMe, was not appropriate.

Contingency plans, emergency plans and verification requirements

37. Due to tight timeframes and costs that may prove prohibitive, there is a risk that the trial may not proceed or that individual councils will withdraw from it. Therefore, participating member councils will require a robust contingency plan in the event of that outcome, and for the event that one or more member councils withdrawing from the trial.
38. There is also potential that the failure of an online voting system could significantly affect a large number of people's ability to vote. Additionally, failure of any of the technical components that make up the online voting service could lead to submitted votes being lost, either individually or on masse.
39. Therefore I recommend that the regulations require that electoral officers establish an effective contingency procedure in place in case of any failure of the online voting system before a CE can signal his approval for a trial. This plan would need to establish sufficient and effective back-up arrangements and appropriately authorise officials to implement the procedure.
40. A contingency plan would also need to establish what actions the electoral officer would take in the event that concerns are raised that the online voting system is not operating in accordance with regulations and technical specifications. This would include how and when a trial would be suspended, and what steps the electoral officer would take to inform the electorate.

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

Electors will need to authenticate their identity using a unique access code and a secondary method to be determined by member councils

41. Online voting and the democratic process in general, could be seriously undermined if certain individuals are able to impersonate other individuals and vote on their behalf. Under this proposal, electoral officers would be required to advise each elector of a unique access code for the online voting solution at the same time as they issue voting papers by post.
42. The current postal method has no additional means of authentication, but rather relies on the possession of the ballot paper, people behaving ethically and lawfully and the trustworthiness of the postal system. However, due to the additional risk of large scale fraud or disruption associated with online voting, a higher standard of security is required. Online voting also presents opportunities for additional security and greater control than are practical for postal-voting. I therefore recommend that regulations require a second authentication process be used in a trial.
43. In order to succeed in New Zealand, online voting will need to reconcile the tension between authentication requirements (which must be linked to the electoral roll) and ease of access for voters. There are several available options for a secondary authentication tool, including:
 - 43.1 mail-out of a secondary user access code to electors;
 - 43.2 use of a 'shared secret', that is known only to the voter and the online voting system (e.g. date of birth);
 - 43.3 pre-registration for the online voting trial to enable more secure authentication of the voter; or
 - 43.4 use of RealMe as a secondary authentication tool.
44. All of these options have strengths and weaknesses. Both a secondary mail-out and a shared secret using date of birth information would make online voting highly accessible and are more secure than postal voting. However, while it is less likely that two separate letters will be intercepted, this option is still vulnerable to all the shortcomings of the postal-voting system and will significantly increase cost. Further, ~~a~~an elector's date of birth could still potentially be accessed ~~discovered~~ by a third party (e.g. through social media). By combining a random code printed on the voting papers with the elector's knowledge of their date of birth attempts to subvert voting en masse are substantially reduced.
45. By comparison, pre-registration (either through a trial specific mechanism or RealMe) would offer significantly more secure authentication of the voter, and has frequently been an element of successful overseas online voting systems. However, pre-registration represents a significant barrier to uptake of online voting as it requires an active engagement by electors to register. As such there is a risk that a trial involving pre-registration will have lower uptake and that it will be less representative.

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

46. Given that each option has clear strengths and weaknesses, I recommend that local authorities be given the discretion to determine the secondary authentication tool that they consider best meets the needs of their trial, rather than prescribing a specific method in regulations. This way, member councils can work in partnership with central government and service providers to determine which option best balances security, accessibility and privacy, whilst still meeting the goals of their trial. For simplicity and ease of evaluation, all members of the working group will be required to utilise the same secondary authentication method.
47. It is worth noting that the Local Electoral Act states that date of birth information can only be accessed by electoral authorities if explicitly required by regulations. The Department will look to work in partnership with member councils to test whether this is the preferred approach to implementing a secondary authentication tool (see discussion on the release of an exposure draft below). If this is the preferred approach I will seek approval for this approach when final regulations are submitted for Cabinet approval in early 2019.

The results of an online election need to be independently verifiable and voters should be able to determine if their vote was recorded as cast

48. One of the core principles of the Local Electoral Act is the adoption of voting mechanisms that are transparent and that produce certainty of the fairness and accuracy of the vote. Given that there is no history of online voting in public elections in New Zealand, this may increase the likelihood that the electoral processes or results are disputed. Without a mechanism in place to ensure that votes in the electronic ballot box contain a complete and accurate record of votes cast, there is a significant risk that public trust in the online trial will fail.
49. Therefore I recommend that regulations require that any online voting solution includes the necessary procedural and technical controls to ensure that the results can be independently verified if they are disputed. This would include a requirement that, in the event of a recount, the necessary records of the unencrypted votes be securely held until the recount is completed.
50. An additional question is whether it should be possible for individual voters to verify whether their vote was recorded as it was cast. Again, this sets a higher standard than currently exists for postal voting. Further, providing the voter with verifiability while maintaining voter privacy can be a difficult objective to meet.
51. However, again given the importance of maintaining elector confidence, I consider that some form of voter verification is a necessary prerequisite for the current trial (though this may not necessarily be a requirement in the longer term). I therefore recommend that the regulations specify that all participating electoral officers must, at the request of a voter, be able to allow the voter to inspect how their vote has been recorded.

In the event of multiple votes, both votes will be invalidated

52. In some overseas jurisdictions, online voting trials have allowed for multiple votes to be cast, with the last vote being the decisive one. Other overseas trials have been undertaken on the basis that any postal vote will override an online vote.

Commented [AJ55]: Not necessarily unencrypted, but if encrypted it is critical that the encryption keys are properly handled

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

53. Current rules in New Zealand set out that in the event of multiple voting at the same time invalidates both votes, unless the Electoral Officer is satisfied that one of the two votes is legitimate. I recommend that the default be that this approach is retained in the event of an online trial. Establishing which out of a postal or online vote was issued last, or instituting rules that require postal voting to override online voting will add additional complexity both technically and procedurally. Therefore, as a default, I recommend that the status quo apply to duplicate votes, and that this process be effectively communicated to voters through issued voting papers.

Partial trials as a way of reducing risks and costs

54. Additionally, it may be necessary for local authorities to undertake 'partial trials' of online voting within their electorates. This may be the case where the electorate is particularly large (e.g. Auckland) and it is considered that the risks and costs of a failure of the online trial are too significant and will affect too many potential voters. For this reason I recommend that no more than one third of the electors within a local authority be eligible to participate in the trial. It is also possible that electorates may wish to trial online voting as a means for improving accessibility to people with disabilities (e.g. the blind) or who live overseas.
55. I therefore recommend that regulations provide for each local authority within the working group to specify a subset of voters to participate in an online voting trial. Regulations would allow these subsets of voters to be specified by reference to:
- 55.1 a local government area or subdivision in which the specified class of electors is eligible to vote; or
 - 55.2 any other characteristic that makes a voting method suitable for the specified class of electors (e.g. the members of the specified class may reside overseas, or have a relevant disability).

An evaluation of the trial is a necessary requirement to inform the development of online voting

56. Finally, it is intended that a trial inform future policy decisions in relation to the future conduct of online voting in local elections. It is therefore necessary that the member councils make provision to fund an independent evaluation of the trial. The evaluation would apply a consistent methodology in evaluating the experiences of different members, including, amongst other aspects:
- 56.1 whether the online voting system was secure (and whether it was perceived to be secure), private and accurate;
 - 56.2 how available the electors found the online voting system to be, how accessible the user experience was, and who used it;
 - 56.3 whether local authorities effectively identified and managed the risks associated with the delivery of online voting services;
 - 56.4 what, if any, outcomes were achieved by the introduction of an online voting system over and above current postal voting; and
 - 56.5 whether the regulatory framework established for the trial was fit for purpose.

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

Risks with the proposal to be considered

DHB's are unlikely to be able to commit funding to support a trial

57. The Local Electoral Act 2001 determines that for a triennial election, the voting method(s) to be used by all entities (including District Health Boards) in the relevant territorial authority's area is the voting method adopted by the territorial authority. Therefore, under the current legislation if member councils choose to adopt online voting, this method must also be made available for DHB elections.
58. The Local Electoral Act requires that the entities involved in a triennial election must pay the "reasonable costs and expenses incurred...as agreed by...the local authorities concerned". In practice, this has resulted in the costs of triennial elections being shared between the respective parties, usually via a contractual agreement prepared by each territorial authority and agreed in advance. If agreement cannot be reached regarding cost sharing, the Office of the Auditor General has responsibility for settling disputes.
59. The member councils have signalled that they anticipate the usual cost-sharing arrangements between participant entities would apply for an online voting trial. However, DHB's are already financially stretched, and are unlikely, individually to be able to commit the additional funding required for the trial. This potentially creates a risk as if cost sharing agreements cannot be reached, and no additional funding is available, this could prevent some councils from participating in the trial.

My officials will review options for ensuring that the trial is effectively resourced

60. As noted above, central government has an interest in the integrity of the local electoral system. The success of an online voting trial is important to ensuring that local elections remain fit for purpose in the medium term. A lack of sufficient resourcing (amongst local authorities, regional councils and DHB's) could significantly affect the quality of the online voting solution and the extent of the trial. I will consider options for ensuring the trial is effectively resourced, and if necessary, report back to Cabinet in due course.
61. I will only be able to give an indication of the likely cost of the trial once the member councils have each issued a Request for Proposal (RFP). The cost could be a significant barrier to the success of the trial.

Councils have strong incentives to effectively manage the risks of online voting

62. The approach taken in 2016 was concerned with minimising a number of risks related to the conduct of an online voting trial. These included risks to:
 - 62.1 the integrity (including perceived integrity) of the election process and election result if the trial failed or was poorly managed;
 - 62.2 public confidence in online voting systems, or online transactions generally, if the online component failed or was hacked, or security or privacy was breached; and
 - 62.3 political reputation for both councils and Government if trials were perceived to have failed or been poorly managed.

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

63. While these risks are real, I do not believe it is appropriate to attempt to manage them through a regulatory approach. Several member councils, including Auckland Council, are large, sophisticated and well-resourced with considerable technical and managerial expertise. Many of its transactions with citizens are conducted online and it wishes to expand and improve this interface. The incentives it faces to ensure effective management of identified risks are significant and likely to be more effective than a regulatory approach. Other members of the working group will also benefit from Auckland's expertise and resources.

Next Steps

I seek agreement to release an exposure draft to test the regulatory framework with sector stakeholders

64. In order to effectively progress the design of the regulatory framework, and to support the development of an effective online voting solution, it will be necessary to develop an exposure draft of the proposed regulations and consult closely with member councils.
65. This exposure draft will include provisions addressing a number of minor policy issues. These issues are not significant matters of policy. They largely involve generic provisions for the conduct of voting, equivalent to currently existing regulations for postal voting in the Local Electoral Regulations 2001. Additionally, the exposure draft will include some consequential provisions that result from the policy decisions sought in this paper (e.g. publicity requirements, processes for elector feedback, processes for when an elector loses their access code etc.). I therefore seek Cabinet authorisation to release an exposure draft that resolves these minor policy issues.
66. The exposure draft will be public, and the Department will invite submissions from a subset of stakeholders including the member councils, LGNZ, SOLGM, key academics, industry stakeholders and potential online voting service providers.
67. If you agree to my proposal, my officials will begin work on the development of an exposure draft of the regulatory framework to be released for selective consultation in late September for a period of four weeks.

Given other priorities in the Local Government Portfolio, my preferred approach is that work on the review is put on hold

68. Given other priorities within the local government work programme (including supporting Select Committee hearings of submissions and consideration of the Local Electoral Matters Bill), developing an exposure draft will require that the wider Review be put on hold for the development of regulatory framework for online voting trials (though the Bill will proceed). The objectives and scope of the Modernising Voting Review were developed in consultation with LGNZ and SOLGM, and the review remains a high priority for these stakeholders and the wider local government sector.
69. There is a risk that delaying the review could negatively affect trust between government and the sector, on matters relating to the online voting trial and the wider local government work programme. My officials will seek to mitigate this risk by working closely with LGNZ, SOLGM and other local government stakeholders to establish that the Review remains a priority for the Government, and that it will resume once work on finalising the regulatory framework for online voting trials is complete in early 2019.

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

70. Once drafting of the regulations is completed, I will return to Cabinet in early February 2019 to receive Cabinet approval, in order for the Regulations to be promulgated in March.

Consultation

71. This paper was prepared by the Department of Internal Affairs in consultation with...
72. The following agencies were provided draft versions of this paper for consultation:

Financial implications

73. There are no financial implications of this paper for central government. The establishment of a regulatory framework will precipitate the release of an RFP by member councils that will provide an indication of the likely cost to local authorities of undertaking a trial.

Human rights and gender implications

74. There are no human rights or gender implications arising from the proposals in this paper.

Disability perspective

75. The development of online voting could assist the visually impaired and other disabled people to vote independently. Disability advocacy groups will be consulted as part of the development of any online voting trial.

Legislative implications

76. <insert text>

Regulatory impact analysis <remove if not required>

77. Tbc

Publicity

78. I expect that the member councils will be responsible for developing a comprehensive communications strategy for the online voting trial, and that communications and engagement with the public will primarily be a sector responsibility.

Recommendations

79. The Minister of Local Government recommends that the Cabinet Economic Development Committee:
1. note that on 21 March 2018, the Cabinet Economic Committee agreed that the Local Electoral Act 2001 be amended to enable regulations to be promulgated authorising a local authority to adopt a voting method for a specified subset of electors at an election, for the purposes of trialling a voting method (DEV 18 Min 022 refers);
 2. note that the Local Electoral Matters Bill (the LEM Bill) which will give effect to the decision in 1 above (and related policy decisions) has been introduced and is currently before the Justice Committee with a report back date of 9 November 2018;

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

3. **note** that when agreement to the LEM Bill was sought, I signalled that I would report back to Cabinet regarding a trial(s) of online voting, including the content of regulations to authorise online voting trials and consideration of the financial implications of any such trial.
4. **note** that further work between the Department of Internal Affairs, Local Government New Zealand and the NZ Society of Local Government Managers has concluded that a nationally coordinated and managed online voting trial in 2019 is not feasible with current timeframe and resourcing;
5. **note** that a group of councils has agreed in principle to an online voting trial at the 2019 local elections, subject to (amongst other matters) the passage of the (the LEM Bill) and the promulgation of an enabling regulatory framework;
6. **note** that, in order to enable trials of online voting as soon as possible, enabling regulations will need to place responsibility for ensuring the integrity and security of elections at which trials are conducted on the local authorities
7. **agree** that the proposed enabling regulations apply only to local authorities that choose to join a working group of councils, to be specified in regulations;
8. **agree** that the proposed enabling regulations apply only to the 2019 triennial local authority elections and any interim elections (e.g. local by-elections and referenda) that take place prior to the 2022 elections;
9. **agree** that the proposed enabling regulations should give effect to the following requirements:
 - 9.1 Online voting may be made available to a subset of enrolled electors at any election, by-election or poll conducted by a territorial authority as an alternative to casting a postal ballot
 - 9.2 A subset of electors may be specified by:
 - 9.2.1 a local government area or subdivision in which the specified class of electors is eligible to vote; or
 - 9.2.2 any other characteristic that makes a voting method suitable for the specified class of electors (e.g. the members of the specified class may reside overseas, or have a relevant disability).
 - 9.3 Access to online voting must require an authentication system, based on:
 - 9.3.1 a unique access code mailed to the elector at the same time as postal voting papers are issued; and
 - 9.3.2 a secondary system that effectively ensures the secrecy, security, accuracy, reliability and accessibility of the online voting system
 - 9.4 Before adopting the online voting method authorised by the regulations under section 36, the local authority must first receive a published report from the Chief Executive advising of his/her satisfaction that the proposed solution is:
 - 9.4.1 secret, so that data is stored in a way that prevents any person from being able to associate a vote to an individual without that individual's consent;
 - 9.4.2 accurate, so that the vote cast accurately reflects the intentions of the voter and is recorded as such;

Commented [AJS6]: In combination with something unique to and already known to each elector, e.g. date of birth

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

- 9.4.3 available and reliable, so that the system performs as intended and an individual can cast their vote at all times that postal voting is also available;
 - 9.4.4 auditable, so that the electronic ballot box can be reviewed in the event of a recount or a disputed vote;
 - 9.4.5 verifiable, so that it is possible to verify that the electronic ballot box contains a complete and accurate record of the votes cast; and
 - 9.4.6 secure so that the solution complies with relevant New Zealand and international security standards and includes documented incident response plans.
- 9.5 that the technology and procedures to be used are independently audited to assess whether they are fit for purpose and meet the requirements of these regulations;
 - 9.6 that the operation of the voting and counting mechanisms and procedures used is auditable, and that the results of the election are capable of independent verification;
 - 9.7 that local authorities must, at the request of a voter, be able to allow the voter to inspect how their vote has been recorded;
 - 9.8 that robust contingency procedures are in place to manage the impact of any technical or other problem with the conduct of the election;
 - 9.9 that in the event that multiple votes are recorded from the same elector, both votes are invalidated;
 - 9.10 that participating councils will undertake an evaluation of the trial to assess the effectiveness of the online voting solution and the regulatory framework;
10. agree that, in order to enable trials of online voting as soon as possible, the Minister of Local Government authorise drafting instructions be issued;
 11. note that the Minister of Local Government intends to approve the release of an exposure draft of the enabling regulations, in accordance with the Attorney General's protocol, be available as early as is practicable in anticipation of the enactment of the legislation and in accordance with high level policy decisions sought above;
 12. authorise the Minister of Local Government to make detailed policy decisions concerning the drafting of the exposure draft of the proposed regulations consistent with the general approach and policy direction outlined in this paper;
 13. agree that, in order to enable trials of online voting as soon as possible, officials prioritise supporting the passage of the legislation and development of enabling regulations over progressing wider aspects of the modernising voting review, including finalising the terms of reference, scope and timeframe for the wider Review;
 14. Agree that the Minister of Local Government will seek confirmation of the final policy content of enabling regulations following consultation on the exposure draft.

Commented [KS7]: This is slightly inconsistent with para 53, which recommends both votes be invalidated "unless the Electoral Officer is satisfied that one of the two votes is legitimate".

IN-CONFIDENCE – NOT OFFICIAL GOVERNMENT POLICY

Authorised for lodgement

Hon Nanaia Mahuta

Minister of Local Government

Released under the Official Information Act 1982

Kate MacDonald

From: 9(2)(a)
Sent: Friday, 27 July 2018 9:48 AM
To: 9(2)(a)
Subject: RE: Debrief from Online Voting Brief, Chirstchurch 19 July

Thanks 9(2)(a)

I'm very much in support of work continuing towards a successful trial of online voting. It is regrettable that momentum was lost after the unsuccessful effort leading up to the 2016 elections, and I'm pleased that the councils are continuing to push towards a trial, albeit with reservations about the practicalities of driving towards a 2019 local body elections target. My thought is that the best outcome would be that a trial is both successful and establishes a foundation for future online elections. As you say the biggest risk is that an unsuccessful trial could undermine public confidence in future efforts to introduce online voting in local or national elections. The second risk that concerns me is that a rushed effort, even if successful as far as election outcomes are concerned, may not provide insight into how this could be adopted post-trial.

It was my assessment earlier this year that between the councils, local government representative bodies and central government we still lack the expertise necessary to properly understand the requirements for online voting. If the councils maintain their determination to issue the RFP in September I think it's unlikely that the requirements will be well understood. I'd prefer to see a properly resourced project established as soon as possible to work on identifying the requirements for a longer-term online voting solution as well as the trials, and to continue working towards a series of trials after the 2019 elections. Pragmatically, from where we are today the two paths to success as I see them are:

1. Between the councils and central government we meet the target to confidently run trials of online voting in the 2019 local body elections, or
2. The councils recognise that they are unlikely to be ready to meet the 2019 target and re-focus work to achieve a good quality trial for a by-election or non-binding referendum.

With the councils currently focussed on the former our best chance for success is to support them as much as we're able, and to hope that all parties are open to reassessing this approach as progress is made.

9(2)(a)

From: 9(2)(a)
Sent: Thursday, 26 July 2018 10:34 PM
To: 9(2)(a)
Subject: RE: Debrief from Online Voting Brief, Chirstchurch 19 July

Thanks for this 9(2)(a) I will say my interest for putting my hand up for this work is I think there's an opportunity for something to happen here that would be really good for NZ, but more so there's considerable risk for something to derail a broader future opportunity.

I'm very aware (and will hopefully frame this over coming weeks) that it's not clear what our role is, both within the Department and with Local Government, so the first thing I'm keen to do is ensure we all get on the same page there and then make sure we position ourselves so we can provide the best support we can to make sure this pilot / trial has the highest integrity – if it goes ahead.

My gut feel is the timeframe that is being talked about is really tight, but that in itself is not a reason to not proceed. My biggest concern is not that this work isn't successful, rather what a failure would have on the concept going forward on a larger scale.

Anyway, I think we are catching up for the first time tomorrow and the next few weeks should be quite interesting as we develop what our roles are and how we best position ourselves to support both this work with Policy and the Councils, but also Ministers, going forward.

Cheers

9(2)(a)

OUT OF SCOPE

OUT OF SCOPE

OUT OF SCOPE

OUT OF SCOPE

OUT OF SCOPE

Released under the Official Information Act 1982

OUT OF SCOPE

Released under the Official Information Act 1982

9(2)(a)

From: 9(2)(a) (a)
Sent: Thursday, 4 October 2018 12:44 PM
To: 9(2)(a)
Cc: 9(2)(a)
Subject: RE: Online voting - advice or contact for standards on secure operations

Hi 9(2)(a)

I'm happy to discuss this with you. In general I've recommended focussing on outcomes rather than specific technical controls as the specifics tend to become outdated rather quickly.

I'm away on leave next week. I can meet with you after 3:30 today or any time that's free in my calendar tomorrow.

Regards,

9(2)(a) | 9(2)(a) - 9(2)(a)
Te Kōtūi Whitiwhiti | Service & System Transformation (SST)
Level 11, 45 Pipitea Street | Mobile 9(2)(a) | www.dia.govt.nz

From: 9(2)(a)
Sent: Thursday, 4 October 2018 11:02 AM
To: 9(2)(a)
Cc: 9(2)(a); 9(2)(a)
Subject: RE: Online voting - advice or contact for standards on secure operations

Hi 9(2)(a)

As discussed I think the answer to your question regarding the security etc. of the data is addressed by the classification that is given to the data and the retention / disposal would presumably be consistent with what the paper based is (i.e. time period etc).

Encryption is a step to address a security concern and links back in my mind to the classification.

I would re-iterate my bigger concern is the linking of the individual to the vote itself, and the confidence that it is the right person voting, and while I understand the process is likely of no greater risk than the current off-line process I am worried about the public perception on this and how it may be portrayed, and in turn what that might lead to in confidence in on line voting full stop.

I've copied 9(2)(a) (a) on this email as 9(2)(a) has been providing the technical advice on this engagement to date and I think is the most qualified of our team to help answer your questions.

9(2)(a) are you able to engage with 9(2)(a) on this to provide some guidance please, as I've noted above I don't think we are talking about creating a whole new set of requirements around on-line voting but if you have a different view on that lets get it on the table. Otherwise it might be providing some advice on where 9(2)(a) can confirm some of the details he needs.

Cheers

9(2)(a)

From: 9(2)(a)
Sent: Thursday, 4 October 2018 8:59 AM
To: 9(2)(a)

Subject: RE: Online voting - advice or contact for standards on secure operations

Importance: High

Hi [9(2)(a)]

Further to the email below, I also need to speak to someone about another couple of aspects of online voting asap

We are looking to advice PCO in the coming days about:

- Content about security, custody, disposal of the online voting system and data.
- Whether levels of encryption should be specified in the exposure regulations.

Thanks

[9(2)(a)]

From: [9(2)(a)]

Sent: Wednesday, 3 October 2018 4:25 PM

To: [9(2)(a)]

Cc: [9(2)(a)]

Subject: Online voting - advice or contact for standards on secure operations

Importance: High

Hi [9(2)(a)]

As you may know, Policy are working on Local Electoral Online Voting Amendment Regulations. This to issue exposure regulations later this month.

We are hoping you can direct us to someone who can provide advice about standards for secure operation of online voting systems.

We anticipate the regulations will say something along the lines of the "the solution provider should provide evidence that the solution and operation of the solution have been tested and proven to meet appropriate standards for secure operation, such as ...".

SST's advice about potential standards to use in the regulations would be very useful.

We are operating to tight timeframes for these exposure regulations, so it would be great if you could get back to me shortly.

Thanks

[9(2)(a)]

[9(2)(a)]

[9(2)(a)]

The Department of Internal Affairs Te Tari Taiwhenua

Direct Dial: [9(2)(a)] [9(2)(a)]

45 Pipitea Street | PO Box 805, Wellington 6140, New Zealand | www.dia.govt.nz

From: 9(2)(a)(a)
Sent: Thursday, 4 October 2018 4:56 PM
To: 9(2)(a) 9(2)(a) 9(2)(a)
Cc: 9(2)(a)
Subject: RE: Security and disposal of records discussion

Something I forgot to mention; I had some concerns about the authentication method that was proposed at the time I reviewed the draft Cabinet paper Minister Mahuta was to present earlier this year. I'd like to have a quick look at how this is being drafted just in case some issues remain.

Regards,
- 9(2)(a)

From: 9(2)(a)(a)
Sent: Thursday, 4 October 2018 4:32 PM
To: 9(2)(a) 9(2)(a) 9(2)(a)
Cc: 9(2)(a)
Subject: RE: Security and disposal of records discussion

Link to draft recommendations as discussed.

<https://dia.cohesion.net.nz/Sites/GCIO/AOGA/layouts/15/DocIdRedir.aspx?ID=4UAZY7VS6QRJ-101908526-28>

9(2)(a)

-----Original Appointment-----

From: 9(2)(a)
Sent: Thursday, 4 October 2018 1:04 PM
To: 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)(a)
Cc: 9(2)(a)
Subject: Security and disposal of records discussion
When: Thursday, 4 October 2018 3:30 PM-4:00 PM (UTC+12:00) Auckland, Wellington.
Where: 9(2)(a)

From: 9(2)(a)
Sent: Monday, 13 August 2018 2:25 PM
To: 9(2)(a)
Cc: 9(2)(a); 9(2)(a)
Subject: RE: On-line voting requirements

Follow Up Flag: Follow up
Flag Status: Completed

Hi 9(2)(a)

Sorry I couldn't make it on Wednesday. I've got some comments below. Please let me know if you want to discuss.

General comments

1. It doesn't appear they've carried out a privacy impact assessment on the proposal, which is a pretty big step to have missed. If they plan to do one later in the process, it's likely to be too late to change anything they've missed. For a system of this level of constitutional importance they really need to ensure they tick all the boxes. I strongly suggest a PIA be carried out before going to RFP. We can suggest some contractors for this if they can't do it in house.
2. I can't see a requirement that deals with fraudulent registrations – eg. someone going through the electoral roll and enrolling everyone they can find. I think there needs to be something about detecting multiple registrations against the same band form of communication (eg 30 registrations against one mobile number). But this can't be absolute – families do share email addresses, mobiles, IP addresses etc.
3. **NFR-033** – Discusses the GCIO. Suggest it be changed to the GCDO. The security document does the same thing.
4. **NFR-037** – States that "*Data to be accessed/processed/stored per NZ privacy framework standards (or stronger). Privacy of individuals must be maintained and guaranteed against any possible system failure.*" I know that this hasn't come from DIA, but could you let me know what this framework is? In the related security pdf, it states:

2.42 The legal jurisdiction in which the data would be accessed / processed / stored must have similar or stronger privacy framework than that of New Zealand.

2.43 The service provider must provide information security controls to meet the adequate level protection requirements dictated by the local privacy laws, where the data would be accessed / processed / stored.

These are different from what's in the RFP itself, and I think they've gotten these requirements from another project document, as they don't really make sense in this context. Firstly, no-where does the RFP require the system to be compliant with the NZ Privacy Act, and secondly, most of the governance of electoral rolls and voting is under the Electoral Act, not the Privacy Act. Normally clauses like 2.42 and 2.43 above are about enabling people to complain to local privacy enforcement bodies where there information has been misused etc. I can't think of any scenarios where you'd do this in relation to electoral information, as either the electoral commission or police are the appropriate bodies.

Happy to talk to Auckland Council about this if it would help?

5. **ADD-PEND-002** – Requires passport or DL number to register online. This is a more onerous process than for mail electors, or electors at national elections. In both cases ID isn't required. As this is a blueprint for future elections, suggest people be able to enrol without providing ID (as this excludes a portion of potential

voters). Could have a system where people could register to vote online, then get sent something to complete the enrolment. This is just as secure as in person voting (where you just take your easyvote card, which is sent to you, or simply tell them your name and address), or the existing mail voting system. It also adds in the Postal Act safeguards (illegal to open another's mail) that I think the .

6. **NFR-017 and ADD-PEND-003** – Might be worth clarifying that the two pieces of information provided by the person enrolling for online voting as in ADD-PEN-003 does not amount to the two-factor authentication required in NFR 017.

Thanks,

9(2)(a)

9(2)(a) Senior Advisor to the Government Chief Privacy Officer | Service and System Transformation
Department of Internal Affairs | Te Tari Taiwhenua

Direct Dial: 9(2)(a)

www.dia.govt.nz

Please note I do not work Wednesdays

From: 9(2)(a)

Sent: Monday, 13 August 2018 10:50 AM

To: 9(2)(a)

Cc: 9(2)(a)

Subject: On-line voting requirements

Hi all

Following on from our meeting last week did anyone have any feedback on the requirements that we were provided, I have heard from 9(2)(a) but no one else yet (unless I've missed your emails, in which case I apologies).

Can I have a response today please.

Cheers

9(2)(a) General Manager | Service Innovation

The Department of Internal Affairs Te Tari Taiwhenua

Direct Dial: 9(2)(a)

Level 10, 45 Pipitea Street, PO Box 805, Wellington 6140, New Zealand



Te Tari Taiwhenua
Internal Affairs

From: 9(2)(a)
Sent: Tuesday, 17 July 2018 4:07 PM
To: 9(2)(a)2(a)
Cc: 9(2)(a)(a)
Subject: RE: Local government e elections

Follow Up Flag: Follow up
Due By: Wednesday, 18 July 2018 8:30 AM
Flag Status: Flagged

Thanks 9(2)(a)

I've only really had time to give the paper a quick once over, so apologies if some of the comments below are a little half formed.

9(2)(a) if there is anything below which doesn't make sense get in touch and I'll be happy to clarify.

The general intention to replicate the existing framework to allow for digital voting is sensible and will hopefully facilitate easier uptake by local authorities.

33.1 – this risk mitigation states a requirement for there to be no capacity for a vote to be associated to an individual without their consent.

Of key importance here is whether this is a capability which currently exists without individual action.

Under the current postal vote system, is there any way for a physical ballot to be associated to an individual without a direct action by that individual to enable the association?

This question is beyond me giving consent. The query is whether my physical ballot paper could be associated to me without my consent (albeit unlawfully), or whether I would need to contribute some piece of information before it could possibly happen.

If the answer is No (association could not happen without my direct action), then the digital arrangement should replicate this. I am wary of creating a scenario where a local authority could bury consent somewhere in the online voting process and then associate all voting records.

Paragraph 36

Could we please call out in here the need for a Privacy Impact Assessment? This is a significant volume of personal information and the majority of the risks identified relate to public perception and social license. Let's be very clear that we will be running a strong privacy lens over this work.

43.4 – use of RealMe for voter authentication

Looking at the objective, this may only be met through a verified RealMe identity. Not many people have a verified RealMe account (though with the introduction of online application we are expecting this to go up). At present, it is likely to be viewed as a barrier rather than a potential solution.

Nō reira,
 Nāku iti nei,
 Nā 9(2)(a)

9(2)(a) | Principal Advisor Privacy | Information and Safety
 Department of Internal Affairs Te Tari Taiwhenua
 Direct Dial 9(2)(a) | Mobile 9(2)(a)



Te Tari Taiwhenua Internal Affairs

From: 9(2)(a)
Sent: Tuesday, 17 July 2018 11:34
To: 9(2)(a)
Cc: 9(2)(a)
Subject: Local government e-elections

9(2)(a)

As discussed, I think you should also probably be aware of these papers. I have let 9(2)(a) know I am passing them on to you. I have also included 9(2)(a) first thoughts on the papers.

Can we get together later today and see what joint concerns we might have?

Thanks

9(2)(a)

9(2)(a) Principal Advisor to the Government Chief Privacy Officer
The Department of Internal Affairs Te Tari Taiwhenua
Direct Dial: 9(2)(a) 9(2)(a)
45 Pipitea Street | PO Box 805, Wellington 6011, New Zealand
www.dia.govt.nz



Te Tari Taiwhenua Internal Affairs

Kate MacDonald

From: 9(2)(a)
Sent: Wednesday, 18 July 2018 9:26 AM
To: 9(2)(a)
Subject: FW: e-voting paper

Section 123 of the LEA will also be relevant *Offences in respect of official documents*
[http://www.legislation.govt.nz/act/public/2001/0035/latest/DLM94787.html?search=ta act L ac%40ainf%40anif an%40bn%40rn 25 a&p=2](http://www.legislation.govt.nz/act/public/2001/0035/latest/DLM94787.html?search=ta+act+L+ac%40ainf%40anif+an%40bn%40rn+25+a&p=2)

and 249, 250 and 252 of the Crimes Act *Crimes Involving computers*
[http://www.legislation.govt.nz/act/public/1961/0043/latest/DLM330415.html?search=sw 096be8ed816b3016 computer 25 se&p=1&sr=1](http://www.legislation.govt.nz/act/public/1961/0043/latest/DLM330415.html?search=sw+096be8ed816b3016+computer+25+se&p=1&sr=1)

From: 9(2)(a)
Sent: Wednesday, 18 July 2018 9:08 AM
To: 9(2)(a)
Cc: 9(2)(a)
Subject: e-voting paper

9(2)(a)

I have a concern about the paper beyond the usual recommendations about privacy impact assessments and the rest. I copied you on 9(2)(a) comments so I will not repeat them. I believe that 9(2)(a) already answered 9(2)(a) question about assurance on privacy?

My concern

The paper does not address penalties for unauthorised or malicious interference with the e-voting processes. Postal voting processes rely on s. 23 Postal Services Act as well as the provisions of the Local Electoral Act to protect the integrity of the voting system. Section 23 is broader in scope and has higher penalties than those under the Local Electoral Act. I am concerned that the proposals in the paper while reassuring about security being taken seriously leave e-votes as a form of second class instrument because of the disparity in penalties that apply.

The relevant sections of the Acts, I mention are below.

Thanks

9(2)(a)

Postal Services Act s23 Unlawfully opening postal article

- (1) Every person commits an offence against this Act who wilfully and without reasonable excuse opens or causes to be opened any postal article that is not addressed to that person.
- (2) Every person who commits an offence against subsection (1) is liable on conviction to imprisonment for not more than 6 months or a fine of not more than \$5,000.

Local Electoral Act

Section 131 Penalty for electoral officer, deputy electoral officer, and other electoral officials

Every electoral officer, deputy electoral officer, or other electoral official commits an offence, and is liable on conviction to a fine not exceeding \$2,000,...

Section 139 regulations

...(l) prescribing penalties for offences against regulations made under this Act, not exceeding a fine of \$2,000:

9(2)(a) Principal Advisor to the Government Chief Privacy Officer
The Department of Internal Affairs Te Tari Taiwhenua
Direct Dial: 9(2)(a) 9(2)(a)
45 Pipitea Street | PO Box 805, Wellington 6011, New Zealand
www.dia.govt.nz



Te Tari Taiwhenua Internal Affairs

Released under the Official Information Act 1982

From: 9(2)(a)
Sent: Wednesday, 27 June 2018 9:04 AM
To: 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
9(2)(a) 9(2)(a)
Subject: RE: Online Voting Local Government: GCDO Support

Hi 9(2)(a)

RealMe is integrated with the Electoral Commission for voter registration, and they were really keen to drive uptake of their online enrolment channel so we could look to engage with them from that perspective to support this? I assume if we are doing online voting we need a way to ensure the identity of the voter and the uniqueness of the vote, RealMe is one way of doing that but we have far from universal coverage of voters, we're sitting at about 450k people (all over 14). We could look at utilising some of the RealMe team that's been working with the Electoral Commission to support this.

In addition to the RealMe angle we could look at utilising some of our service design resource (likely supplemented by bringing some more on which would need to be funded by the project) through the lab to run a sprint to look at options, or we could look at supporting the work at the equivalent in Auckland.

Cheers

9(2)(a)

From: 9(2)(a) 9(2)(a)
Sent: Wednesday, 27 June 2018 8:08 AM
To: 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
Subject: Online Voting Local Government: GCDO Support

Hi

At stand up this week Colin made it clear that he wants GCDO to consider how we can support the trial of online voting for local government elections

The approach has now changed and local government through Auckland City Council will be leading the trial including all design ,build, delivery etc. I have now met with 9(2)(a) and he explained that a light touch regulatory system will be put in place with risk etc sitting with local government. Policy has to send a briefing to the Minister of Local Government next week about the new approach, trial etc and there will need to be a sentence included that likely reads GCDO is considering how they might support the trial.

In the meantime we need to have an agreed view on what that support realistically might look like given its now a local government initiative.

Can you all send me what you consider appropriate for your respective areas by the end of the week so I can pull it into one document for 9(2)(a) in the first instance and then Colin once 9(2)(a) is happy with the approach.

Thanks

9(2)(a)

9(2)(a)
General Manager Strategic Relationships and Advice

Released under the Official Information Act 1982

From: 9(2)(a)
Sent: Tuesday, 17 July 2018 9:20 AM
To: 9(2)(a2)(a)
Subject: RE: Local government e voting paper

Follow Up Flag: Follow up
Flag Status: Completed

Hi 9(2)(a)

Sorry I'm not there in person - give me a bell on my cell if you want to discuss when you come in.

Re: Local government e-voting Cabinet paper

A few possible areas for clarification/addition – quotes from paragraphs in the paper are in black – my comments in blue.

As a general comment, paragraph 36 states that GCDO officials have signalled that they could provide, “advice around security architecture; guidance and a framework for project assurance” etc, do we want to suggest they could also refer specifically to GCPO for privacy assurance considerations?

36. In particular, GCDO officials have signalled that they could provide support and guidance to councils undertaking the online voting trial.

Also, there is no reference in the paper as to whether any insights are/will be gained from Statistics NZ's recent experience with the census online – I would suspect there could be some useful comparators that might provide some useful commentary of both risks and opportunities.

More specific queries/comments as follows

1. This paper seeks agreement to a regulatory approach to enable limited online voting trials in the 2019 local authority elections.

It would be useful to say when the triennial local authority elections are in 2019 – i.e. October – this would help set the scene in terms of the timing pressures.

3. To minimise risks, the regulations will specify that only a subset of councils (members of a planned working group to design and procure an online voting solution) may undertake a trial.

A number of councils have indicated they are considering involvement in the trial. The paper also stresses the pressure on some DHBs that may preclude participation..

However, in terms of potential scope it's not clear whether the regulations will say simply that all local authorities would be eligible (e.g. councils and DHBs) but not all local authorities would need to participate, or would specify who would be involved. Assume it's the former as participation won't be able to be confirmed until after an RFP and full costings have been confirmed which will be at least after the draft regulations have been developed, if not submitted (if they are to be in place by March 2019).

Is there considered to be a minimum viable number for the testing? Of councils/DHBs or both? Would any council/DHB who wished to participate in the working group be excluded in order to “minimise risks”?

10. There are a range of interim options which are currently available to supplement or support the postal. However

Typo - Word "vote" missing after postal

20. Further, delaying a trial would leave time for technical confidence and public acceptance of online voting to grow.

The paper doesn't say anything about public engagement that might help influence public acceptance, only that communications and engagement will be members councils' responsibility (at para 24). (see also comment at para 78 below)

The only specific comment is in terms of preparation of an exposure draft of regulations, nonetheless, it doesn't say how widely circulated that would be, only as per para 76 - that it would involve a four week "selective consultation". With councils? With wider government? Public?

23. I propose that an enabling regulatory framework similar to that for other current voting methods be established.

Would be useful to include examples of the other current voting methods referred envisaged as similar to provide an indication of the practicability and transferability of the proposed approach.

30. several risks pose additional challenges for the successful conduct of an online voting trial, ...

Given the significant privacy risks noted in para 30 (perceived opportunities for malicious interception or a web interface failure; potential for a large privacy breach; risk of challenge to electronic record and lack of paper records for reconstruction/confirmation), would be reassuring if the paper confirmed that the RFP process would entail provision of a Privacy Impact Assessment to show how such risks could be minimised or mitigated through, e.g. the "robust system design, regulatory requirements, assurance auditing, testing and implementation processes" etc referred to in para 31.

33 Therefore, it is necessary that regulations require that before a trial can be conducted territorial authorities first receive a published report from their Chief Executive, advising that they are satisfied that the solution is consistent with a number of desired outcomes.

The risk mitigations that follow in paragraph 33 appear reasonable and comprehensive.

37 Due to tight timeframes and costs that may prove prohibitive, there is a risk that the trial may not proceed or that individual councils will withdraw from it. Therefore, participating member councils will require a robust contingency plan in the event of that outcome, and for the event that one or more member councils withdrawing from the trial.

Typo – withdrawing should read withdraw

40 A contingency plan would also need to establish what actions the electoral officer would take in the event that concerns are raised that the online voting system is not operating in accordance with regulations and technical specifications. This would include how and when a trial would be suspended, and what steps the electoral officer would take to inform the electorate.

Surely requires also means to ensure validity of voting and integrity of result – e.g. if voters try online but the system falls over, they will still want their vote recorded.

50. Further, providing the voter with verifiability while maintaining voter privacy can be a difficult objective to meet.

Firstly, why? (and good reason why a PIA would be recommended). Secondly, the two are not mutually exclusive, but verifiability is a key component of assuring voter privacy.

55 I therefore recommend that regulations provide for each local authority within the working group to specify a subset of voters to participate in an online voting trial. Regulations would allow these subsets of voters to be specified by reference to:

1.1 a local government area or subdivision in which the specified class of electors is eligible to vote; or

1.2 any other characteristic that makes a voting method suitable for the specified class of electors (e.g. the members of the specified class may reside overseas, or have a relevant disability).

How will they decide and keep it representative? How will they know which potential voters might fall within any particular class of disability? (same question applies to the related recommendation 9.2.2)

60 I will consider options for ensuring the trial is effectively resourced, and if necessary, report back to Cabinet in due course.

Cost uncertainties, including who will pay what in any cost-sharing arrangement (given inequity of size/resourcing etc of different local authorities) appear a major potential risk – while the paper is generally clear that local authorities will foot the bill, it is unclear what is envisaged by this statement in paragraph 60, i.e. what other options might be feasible – as this is a project of potentially wide-ranging national significance, if central government is an option this should be stated at least somewhere.

61 I will only be able to give an indication of the likely cost of the trial once the member councils have each issued a Request for Proposal (RFP). The cost could be a significant barrier to the success of the trial.

Multiple independent RFPs? Surely only one from the working group would be involved?

Also, how does this paragraph 60 align with the previous one (paragraph 61) – is cost a risk if councils can't cover the costs r those that can aren't willing to be involved, or is the Minister planning to ensure the trial is effectively resourced?

78 I expect that the member councils will be responsible for developing a comprehensive communications strategy

Typo with the missing gap before "expect".

More substantively though, is this only an expectation?

Given the stress placed in the paper on the importance of maintaining/meeting/ensuring public confidence", "expectations" and "acceptance", and the potential for significant public-funded costs, shouldn't such a strategy be a requirement?

Also, would it be steered by the working group of member councils in a coordinated way, or would each council be responsible for publicity in its own domain?

Rec 9.3 Before adopting the online voting method authorised by the regulations under section 36, the local authority must first receive a published report from the Chief Executive ...

Will this be a standardised format designed by the working group so all CEs are "on the same page" in terms of the assurance and confirmation CEs are providing?

From: 9(2)(a) 9(2)(a)

Sent: Monday, 16 July 2018 11:02 AM

To: 9(2)(a)

Subject: FW: I wasn't sure if I should forward these to you? Is there anything we're contributing?

Please take a quick look at this. See 9(2)(a) cover note for the explanation of why TSS is commenting.

Thanks

9(2)(a)

From: 9(2)(a) 9(2)(a)
Sent: Wednesday, 18 July 2018 9:08 AM
To: 9(2)(a); 9(2)(a)
Cc: 9(2)(a) 9(2)(a)
Subject: e-voting paper

9(2)(a)

I have a concern about the paper beyond the usual recommendations about privacy impact assessments and the rest. I copied you on 9(2)(a) comments so I will not repeat them. I believe that 9(2)(a) already answered 9(2)(a) question about assurance on privacy?

My concern

The paper does not address penalties for unauthorised or malicious interference with the e voting processes. Postal voting processes rely on s. 23 Postal Services Act as well as the provisions of the Local Electoral Act to protect the integrity of the voting system. Section 23 is broader in scope and has higher penalties than those under the Local Electoral Act. I am concerned that the proposals in the paper while reassuring about security being taken seriously leave e-votes as a form of second class instrument because of the disparity in penalties that apply.

The relevant sections of the Acts, I mention are below.

Thanks

9(2)(a)

Postal Services Act s23 Unlawfully opening postal article

- (1) Every person commits an offence against this Act who wilfully and without reasonable excuse opens or causes to be opened any postal article that is not addressed to that person.
- (2) Every person who commits an offence against subsection (1) is liable on conviction to imprisonment for not more than 6 months or a fine of not more than \$5,000.

Local Electoral Act

Section 131 Penalty for electoral officer, deputy electoral officer, and other electoral officials

Every electoral officer, deputy electoral officer, or other electoral official commits an offence, and is liable on conviction to a fine not exceeding \$2,000,...

Section 139 regulations

...(l) prescribing penalties for offences against regulations made under this Act, not exceeding a fine of \$2,000:

9(2)(a) 9(2)(a) Principal Advisor to the Government Chief Privacy Officer
The Department of Internal Affairs Te Tari Taiwhenua

9(2)(a) 9(2)(a)
45 Pipitea Street | PO Box 805, Wellington 6011, New Zealand
www.dia.govt.nz



Te Tari Taiwhenua Internal Affairs

Released under the Official Information Act 1982

9(2)(a)

From: 9(2)(a)
Sent: Wednesday, 18 July 2018 9:45 AM
To: 9(2)(a)
Subject: RE: e voting paper

Agree, but it would be the LEA that would be likely to take precedence over the PSA if there has been an impact on the voting process (rather than simply opening but not interfering with someone else's postal ballot). PSA s23 applies only to opening of mail, whereas altering, stealing, mis-directing etc would be the underlying concerns in terms of electoral process validity and security which would all be covered by LEA for postal votes and by Crimes also for electronic.

From: 9(2)(a)
Sent: Wednesday, 18 July 2018 9:30 AM
To: 9(2)(a)
Subject: RE: e voting paper

Yeah, but people shouldn't have to go look at 5 different pieces of legislation to know what the penalties are. It's a problem now because most people don't know about the penalties around interference with mail.

From: 9(2)(a)
Sent: Wednesday, 18 July 2018 9:26 AM
To: 9(2)(a)
Subject: FW: e-voting paper

Section 123 of the LEA will also be relevant - *Offences in respect of official documents*

[http://www.legislation.govt.nz/act/public/2001/0035/latest/DLM94787.html?search=ta act L ac%40ainf%40anif a n%40bn%40rn 25 a&p=2](http://www.legislation.govt.nz/act/public/2001/0035/latest/DLM94787.html?search=ta+act+L+ac%40ainf%40anif+a+n%40bn%40rn+25+a&p=2)

and 249, 250 and 252 of the Crimes Act - *Crimes involving computers*

[http://www.legislation.govt.nz/act/public/1961/0043/latest/DLM330415.html?search=sw 096be8ed816b3016 co mputer 25 se&p=1&sr=1](http://www.legislation.govt.nz/act/public/1961/0043/latest/DLM330415.html?search=sw+096be8ed816b3016+co mputer+25+se&p=1&sr=1)

From: 9(2)(a)
Sent: Wednesday, 18 July 2018 9:08 AM
To: 9(2)(a)
Cc: 9(2)(a)
Subject: e-voting paper

9(2)(a)

I have a concern about the paper beyond the usual recommendations about privacy impact assessments and the rest. I copied you on 9(2)(a) comments so I will not repeat them. I believe that 9(2)(a) already answered 9(2)(a) question about assurance on privacy?

My concern

The paper does not address penalties for unauthorised or malicious interference with the e voting processes. Postal voting processes rely on s. 23 Postal Services Act as well as the provisions of the Local Electoral Act to protect the integrity of the voting system. Section 23 is broader in scope and has higher penalties than those under the Local

Electoral Act. I am concerned that the proposals in the paper while reassuring about security being taken seriously leave e-votes as a form of second class instrument because of the disparity in penalties that apply.

The relevant sections of the Acts, I mention are below.

Thanks

9(2)(a)

Postal Services Act s23 Unlawfully opening postal article

(1) Every person commits an offence against this Act who wilfully and without reasonable excuse opens or causes to be opened any postal article that is not addressed to that person.

(2) Every person who commits an offence against subsection (1) is liable on conviction to imprisonment for not more than 6 months or a fine of not more than \$5,000.

Local Electoral Act

Section 131 Penalty for electoral officer, deputy electoral officer, and other electoral officials

Every electoral officer, deputy electoral officer, or other electoral official commits an offence, and is liable on conviction to a fine not exceeding \$2,000,...

Section 139 regulations

...(l) prescribing penalties for offences against regulations made under this Act, not exceeding a fine of \$2,000:

9(2)(a) Principal Advisor to the Government Chief Privacy Officer

The Department of Internal Affairs Te Tari Taiwhenua

9(2)(a)

45 Pipitea Street | PO Box 805, Wellington 6011, New Zealand
www.dia.govt.nz



**Te Tari Taiwhenua
Internal Affairs**

9(2)(a)

From: 9(2)(a)
Sent: Thursday, 14 March 2019 11:13 AM
To: 9(2)(a)
Subject: FW: Involvement of GCIO in evaluation panel for online voting - Confirmation needed by COB today

Not "advice" but we did say we can't sit on your evaluation panel and offered some things below, which they didn't take up. They did get some support from CSD in the Security area but once I made the connection I wasn't involved, so you may want to check with 9(2)(a) from there around what they actually did.

And still trolling through my emails.

From: 9(2)(a)
Sent: Thursday, 9 August 2018 9:09 AM
To: 9(2)(a) <9(2)(a)> 9(2)(a)
Subject: RE: Involvement of GCIO in evaluation panel for online voting Confirmation needed by COB today

Hi 9(2)(a)

As discussed yesterday the GCDO is not in a position to provide a resource to sit on the evaluation panel for online voting however we do have part of our business that works in the procurement space that has considerable experience in large multi-agency procurement. Given this is quite a complex area and not necessarily one which people would normally have exposure to we thought that we could offer the Councils advice in a couple of areas:

1. How to best engage with the market to get the outcome you are seeking, and
2. How to setup a suitable commercial model

I'm happy to connect you up to the relevant part of the GCDO if this is of use to you.

That relates specifically to the procurement activity you are looking to undertake, but as you will be aware Cabinet will need to authorise a regulatory approach to enable any online voting trials. Until that occurs, the scope of the GCDO involvement in providing support to councils within the trial can't be determined. However, with these caveats in mind, at this stage I am thinking that we may be able to offer further support in the areas of Assurance and Digital Identity. I'm not clear as to what exactly at this stage so I'm keen to stay in touch as the work progresses to work out how we can be support you.

Regards

9(2)(a)

9(2)(a)

9(2)(a)

The Department of Internal Affairs Te Tari Taiwhenua

9(2)(a)

Level 10, 45 Pipitea Street, PO Box 805, Wellington 6140, New Zealand



**Te Tari Taiwhenua
Internal Affairs**

From: 9(2)(a) [mailto:9(2)(a)]

Sent: Thursday, 9 August 2018 8:43 AM

To: 9(2)(a)

Subject: RE: Involvement of GCIO in evaluation panel for online voting - Confirmation needed by COB today

Good morning 9(2)(a)

Following on our phone conversation yesterday, are you please able to confirm via email the support and collaboration that the online voting working party could receive from GCIO?

Thanks in advance

Ngā mihi

9(2)(a) 9(2)(a)
9(2)(a)
9(2)(a)

Auckland Council, Level 25 135 Albert St, Private Bag 92300, Auckland 1142

Championing engaged, open and innovative democracy and decision-making for the diverse communities of Tāmaki Makaurau

Visit our website: www.aucklandcouncil.govt.nz

From: 9(2)(a) <9(2)(a)>

Sent: Tuesday, 7 August 2018 1:24 PM

To: 9(2)(a) 9(2)(a) <9(2)(a)>

Cc: 9(2)(a) <9(2)(a)> 9(2)(a) <9(2)(a)> 9(2)(a) <9(2)(a)> 9(2)(a)

<9(2)(a)> 9(2)(a)

Subject: RE: Involvement of GCIO in evaluation panel for online voting Confirmation needed by COB today

Hi 9(2)(a)

9(2)(a) spoke to me about this today, I just need to talk to a couple of people and I'll get back to you tomorrow if that's okay.

Regards

9(2)(a)

From: 9(2)(a)

Sent: Tuesday, 7 August 2018 11:54 AM

To: 9(2)(a) 9(2)(a)

Cc: 9(2)(a) 9(2)(a) 9(2)(a)

Subject: RE: Involvement of GCIO in evaluation panel for online voting - Confirmation needed by COB today

Hi 9(2)(a)

As we just discussed the key GCIO contact here 9(2)(a) has been away and he and I was literally just discussing this. I have forwarded this to 9(2)(a) and he will get back in touch with you directly – but it won't be by COP today sorry.

9(2)(a) details are as follows:

9(2)(a) | 9(2)(a) | 9(2)(a)

The Department of Internal Affairs Te Tari Taiwhenua

9(2)(a) 9(2)(a)

Level 10, 45 Pipitea Street, PO Box 805, Wellington 6140, New Zealand

Regards

9(2)(a)
Department of Internal Affairs | Te Tari Taiwhenua
Phone: 9(2)(a) www.dia.govt.nz



Te Tari Taiwhenua Internal Affairs

From: 9(2)(a) 9(2)(a)
Sent: Tuesday, 7 August 2018 11:03 AM
To: 9(2)(a)
Subject: Involvement of GCIO in evaluation panel for online voting - Confirmation needed by COB today

Hi everyone,

We are still waiting on confirmation from you re: the involvement of GCIO in the evaluation panel. Can you please confirm they are happy to be involved and provide us with exact name and contact details for the person who will sit on the panel?

I would appreciate your response by COB today

Thank you

Ngā mihi

9(2)(a)
9(2)(a)
9(2)(a)
Auckland Council, Level 25 135 Albert St, Private Bag 92300, Auckland 1142

Championing engaged, open and innovative democracy and decision-making for the diverse communities of Tāmaki Makaurau

Visit our website: www.aucklandcouncil.govt.nz

From: Elodie Fontaine
Sent: Monday, 6 August 2018 8:51 AM

To: 9(2)(a) 9(2)(a) 9(2)(a)
9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
9(2)(a) 9(2)(a) 9(2)(a)
9(2)(a) 9(2)(a) 9(2)(a)

Subject: FW: Online voting working party - notes & actions from 27 July workshop

Dear all

9(2)(a)

From: 9(2)(a)
Sent: Thursday, 14 March 2019 11:14 AM
To: 9(2)(a)
Subject: FW: Online voting trial 2019

There was this one, and I seem to recall we did give them something small, I'll track that down too.

From: 9(2)(a) | 9(2)(a) <9(2)(a) | 9(2)(a)>
Sent: Wednesday, 22 August 2018 2:04 PM
To: 9(2)(a) | 9(2)(a) <9(2)(a) | >
Cc: 9(2)(a) <9(2)(a) | 9(2)(a) | 9(2)(a)>
<9(2)(a) | 9(2)(a) | 9(2)(a) | 9(2)(a) | 9(2)(a) | 9(2)(a)>
<9(2)(a) | 9(2)(a) | 9(2)(a) | 9(2)(a) | 9(2)(a)>
<9(2)(a) | 9(2)(a) | 9(2)(a) | 9(2)(a)>
Subject: RE: Online voting trial 2019

Thanks 9(2)(a) appreciate your support.

Please do go ahead and set up a discussion and let us know whether you have anyone with the security expertise and availability to advise our evaluation panel. We have the first meeting of the confirmed participating councils on Friday – 9 including Auckland- so we really feel that the trial is getting some traction now. It would be good to be able to update them on any GCIO involvement at the workshop.

Look forward to hearing from you

Kind regards

9(2)(a) | 9(2)(a)

From: 9(2)(a) <9(2)(a) | >
Sent: Tuesday, 21 August 2018 2:37 PM
To: 9(2)(a) <9(2)(a) | 9(2)(a)>
Cc: 9(2)(a) | 9(2)(a) | 9(2)(a)
<9(2)(a) | 9(2)(a) | 9(2)(a) | 9(2)(a) | 9(2)(a)>
<9(2)(a) | 9(2)(a) | 9(2)(a) | 9(2)(a)>
<9(2)(a) | 9(2)(a) | 9(2)(a)>
Subject: RE: Online voting trial 2019

Hi 9(2)(a)

I'm keen to further discuss how we might be able to support you in the areas of assurance and digital identity to support your tender evaluation process, would it be worthwhile me looking to setup a discussion with folk in those areas with the relevance expertise?

More specifically regarding security, and no it doesn't sound like a job description rather it reads like you've given a fair amount of thought to an important area, can I just check that with some of the team here. I'm not sure we actually have that expertise, or if we do to what extent and what it's availability is like. I'll do that as quickly as I can and hopefully get back to you tomorrow.

Cheers

9(2)(a)

From: 9(2)(a) 9(2)(a) 9(2)(a) 9(2)(a)
Sent: Tuesday, 21 August 2018 2:24 PM
To: 9(2)(a)
Cc: 9(2)(a)
Subject: Online voting trial 2019

Good afternoon 9(2)(a)

I am following up on your email to 9(2)(a) dated 9 August regarding the potential role of GCIO in the process for the online voting trial in next year's local body elections. After further discussion with the online voting team, we are interested to explore how we might be able to draw on your expertise in assurance and digital identity to support our tender evaluation process.

Would you have capacity, and would it be appropriate for you, to act in an advisory role during the evaluation period to review the merits of the shortlisted RFPs responses in terms of security? The specifics of what we have in mind are listed below:

- o Review the responses to all requirements and questions related security. We can clearly identify these
- o Identify any gaps, weakness and key differences between the short listed responses
- o Provide this feedback to Auckland Council's ICT representative on the evaluation panel (9(2)(a)) who can then also share this with the other evaluators
- o Be available to discuss your views with 9(2)(a) and/or other evaluators if necessary
- o Highlight questions about the security technologies that we could put to the vendors during their presentations

The kind of expertise we feel we would need to draw on for th s advisory role would be someone with:

- o A proven track record of working full time in information/ cyber security
- o A strong understanding of the security requirements for online voting and the ability to relate these to appropriate security controls
- o Detailed knowledge of the NZISM (NZ Security Information Manual)
- o Knowledge of the CERT NZ Critical Controls 2018 and/ or other international information security frameworks (ISO 27000, NIST, CIS Security Controls).

Apologies if this sounds like a job description, but we are very aware of the importance of this, as I know you will be too.

Please get in touch to discuss the scope of the proposed role. We are very keen to have the government experts play some part in the process at this early stage, as security of the online voting system is a major focus and will have a major impact on public confidence in online voting as an option for future elections.

Kind regards

9(2)(a) 9(2)(a)
[Redacted]
[Redacted]
[Redacted]
9(2)(a)

9(2)(a)

From: 9(2)(a)
Sent: Thursday, 14 March 2019 11:15 AM
To: 9(2)(a)
Subject: FW: Updated comment
Attachments: Proposed authentication approach - jk2.docx; Online voting trial cabinet paper - Final.docx

This is the advice we provided on identity, was via the Policy team

From: 9(2)(a)(a)
Sent: Thursday, 15 November 2018 2:43 PM
To: 9(2)(a) <9(2)(a)Mc 9(2)(a) 9(2)(a) <9(2)(a) 9(2)(a)>
Subject: Updated comment

Hi

9(2)(a) provided me with a cabinet paper (attached) with more detail about their thinking and the options the Solution Provider had to choose from.

I have now updated my comments to align with this. I have not shared this with 9(2)(a) yet in case you wish to add to or moderate it.

Cheers

9(2)(a)

(a) | 9(2)(a) |
Service & System Transformation (SST) Te Kōtui Whitiwhiti
The Department of Internal Affairs Te Tari Taiwhenua
9(2)(a)
45 Pipitea St | PO Box 805, Wellington 6140, New Zealand | www.dia.govt.nz



Te Tari Taiwhenua
Internal Affairs

The Working Party intends to use a pre-registration system.

Note 1

Note 2

A stand-alone registration system is proposed, which would work as follows:

- The voter would pre-register with their name, address and date of birth, which would enable the system to check that they are on the roll
- The voter would also specify their mobile and (not or) email address
- They would then receive a unique PIN by SMS or email
- They would enter that PIN in the system
- The system would then send a confirmation by SMS or email that they are registered.

The Working Party would also like the option of using RealMe credentials to pre-register. They are not 100% sure whether we will offer this option, but their preferred supplier told us that building the interface as the system is developed is much cheaper than doing it afterwards. They think the advantage of offering RealMe as an option is that some voters may find it more secure. Therefore, they would like the regulations to make it possible but not compulsory.

Authentication would then work as follows:

- The voter would enter their access code (found on their ballot paper) into the online voting system
- They would receive an authentication code via SMS or email
- They would enter that authentication code in the system
- They would then be able to vote online.

Note 3

Alternative suggestion

Commented [JK1]: Preamble: My comments are based on the assumption this is local body elections that are currently postal votes and do not identify the voter.

Commented [JK2]: The proposed solution does nothing to mitigate the risk outlined in para 35 of the Cabinet paper

Commented [JK3]: The additional risk posed by the online environment in para 46 relate to the security of the online channel (outlined in para 35) rather than the mechanism by which a voter is authenticated. Therefore the recommendation for a second authentication process is one of perception only.

NOTE: There are no specific requirements or options recommended in the cabinet paper, or any regulations that might contribute to mitigating the risks as outlined in para 35.

Commented [JK4]: Of the 4 options provided for in the Cabinet paper para 47, this is the one most likely to deter people from voting online, thereby failing to address para 31.

Commented [JK5]: The pre-registration and provision of this information is likely to adversely affect the perception of secrecy required in para 38

Commented [JK6]: Adds no value.

Commented [JK7]: Limits online voting to those who possess both a mobile and email. Will there be rules to prevent use of shared phones and/or accounts?

Commented [JK8]: Use of RealMe would not require pre-registration to do so adds a barrier to voting

Commented [JK9]: These steps would not be required if the voter was using RealMe as it would be a repeat.

Commented [JK10]: This proposal seems to be focused on a perception people may have over the security of voting rather than any attempt to increase the likelihood people and ease with which people can vote. It adds a complete new barrier to encouraging people to vote online and does not address the key point of pain - the complexity of local body elections and that they could allow for a save and return.

Commented [JK11]: A better option to meet the perceived requirement that a second level of authentication is needed. Option 2 in para 47 allows for the asking of an additional piece of information that would tie a ballot paper code to a particular recipient. This could be a random question about information already known on the electoral role. An assertion of the FLT from the RealMe login service would also suffice. It could also easily be achieved using analytics, which unfortunately was not a suggested option.

9(2)(a)

From: 9(2)(a)
Sent: Thursday, 14 March 2019 11:16 AM
To: 9(2)(a) 9(2)(a)
Subject: FW: Online voting trial 2019

This was some advice we provided to the council, it was around making sure they had a robust procurement process in place.

From: 9(2)(a)
Sent: Friday, 31 August 2018 1:40 PM

To: 9(2)(a) 9(2)(a)
9(2)(a) 9(2)(a) 9(2)(a)

<9(2)(a)>
Subject: RE: Online voting trial 2019

Hi 9(2)(a)

As part of us working out how we might support the Online voting trial I've engaged a few members of the wider GCDO team here in Wellington and that included some of our all of government ICT procurement folk.

They mentioned to me the other day that they had seen the notice on GETS and they we're just concerned around the process and timeframes, in particular some of the potential challenges involved in setting up an arrangement that may span multiple entities. As you can imagine in their roles they've had quite a bit of experience in multi-agency commercial arrangements.

We had also talked briefly to Paul and the team around Assurance for the work and we've provided some information around what that could look like.

Clearly the advice I've received from my team is based solely on a couple of conversations and what they have seen published on GETS, and they acknowledge that as well. There's likely a whole lot more behind that which we have no visibility of, so the recommendation they've made to me is to suggest that Auckland Council talk to MBIE (as functional lead for Procurement across government) about reviewing the process as it comes under Rule 19 in the Government Rules of Sourcing, which covers risk and cross government initiatives – and that latter presumably applies in a multi agency (in this case Councils) situation. They have told me that they use this review process before they go to market with common capabilities and have found it really useful.

Their key contact they have provided from MBIE is 9(2)(a) he is the Manager Advisory Services, NZ Government Procurement team within MBIE, 9(2)(a)

If it would be useful I'd be quite happy to arrange a conversation directly between our commercial folk and yourself next week, otherwise the engagement directly with MBIE may be useful.

Kind Regards

9(2)(a) | General Manager | Service Innovation
The Department of Internal Affairs Te Tari Taiwhenua

9(2)(a)
Level 10, 45 Pipitea Street, PO Box 805, Wellington 6140, New Zealand



**Te Tari Taiwhenua
Internal Affairs**

From: 9(2)(a) 9(2)(a)
Sent: Thursday, 30 August 2018 5:56 PM
To: 9(2)(a)
Cc: 9(2)(a)
Subject: RE: Online voting trial 2019

Hi 9(2)(a)

Thank you for your email. The best course of action would be to provide any feedback or concerns directly to 9(2)(a) (cc above) 9(2)(a) is Head of ICT & Corporate Procurement and providing Procurement leadership for the Online Voting Trial and would be happy to discuss any questions/concerns and respond accordingly.

Kind Regards

9(2)(a)
9(2)(a)
9(2)(a)

From: 9(2)(a)
Sent: Thursday, 30 August 2018 2:51 PM
To: 9(2)(a) <9(2)(a)>
Cc: 9(2)(a) <9(2)(a)>
Subject: RE: Online voting trial 2019

Thanks 9(2)(a) 9(2)(a) will follow up with you. I am heading overseas for 6 weeks (mid next week) so while I still have Elections programme oversight 9(2)(a) are the key contacts for the online procurement process.

From: 9(2)(a) <9(2)(a)> 9(2)(a)
Sent: Thursday, 30 August 2018 12:04 PM
To: 9(2)(a) <9(2)(a)>
Subject: RE: Online voting trial 2019

Hi 9(2)(a)

Is there any chance you could give me a brief call today 9(2)(a) just in relation to the RFP and a couple of concerns some of the folk here have raised. Really just to flag and discuss, and offer a thought as to connecting in to some expertise at MBIE as part of their Procurement functional lead role.

Cheers

9(2)(a)

From: 9(2)(a) [mailto:9(2)(a)@nz]
Sent: Tuesday, 28 August 2018 7:38 AM
To: 9(2)(a)
Cc: 9(2)(a) 9(2)(a)

From: 9(2)(a) <9(2)(a)>
Sent: Tuesday, 21 August 2018 2:37 PM
To: 9(2)(a) 9(2)(a) <9(2)(a)>
Cc: 9(2)(a) <9(2)(a)> 9(2)(a)
<9(2)(a)> 9(2)(a) 9(2)(a) <9(2)(a)> 9(2)(a) 9(2)(a)
<9(2)(a)> 9(2)(a) <9(2)(a)> 9(2)(a) 9(2)(a)
<9(2)(a)> 9(2)(a) <9(2)(a)>
Subject: RE: Online voting trial 2019

Hi 9(2)(a)

I'm keen to further discuss how we might be able to support you in the areas of assurance and digital identity to support your tender evaluation process, would it be worthwhile me looking to setup a discussion with folk in those areas with the relevance expertise?

More specifically regarding security, and no it doesn't sound like a job description rather it reads like you've given a fair amount of thought to an important area, can I just check that with some of the team here. I'm not sure we actually have that expertise, or if we do to what extent and what it's availability is like. I'll do that as quickly as I can and hopefully get back to you tomorrow.

Cheers

9(2)(a)

From: 9(2)(a) (a)
Sent: Tuesday, 21 August 2018 2:24 PM
To: 9(2)(a)
Cc: 9(2)(a) 9(2)(a)
Subject: Online voting trial 2019

Good afternoon 9(2)(a)

I am following up on your email to 9(2)(a) dated 9 August regarding the potential role of GCIO in the process for the online voting trial in next year's local body elections. After further discussion with the online voting team, we are interested to explore how we might be able to draw on your expertise in assurance and digital identity to support our tender evaluation process.

Would you have capacity, and would it be appropriate for you, to act in an advisory role during the evaluation period to review the merits of the shortlisted RFPs responses in terms of security? The specifics of what we have in mind are listed below:

- o Review the responses to all requirements and questions related security. We can clearly identify these
- o Identify any gaps, weakness and key differences between the short listed responses
- o Provide this feedback to Auckland Council's ICT representative on the evaluation panel (Gaik Lim) who can then also share this with the other evaluators
- o Be available to discuss your views with Gaik and/or other evaluators if necessary
- o Highlight questions about the security technologies that we could put to the vendors during their presentations

The kind of expertise we feel we would need to draw on for this advisory role would be someone with:

- o A proven track record of working full time in information/ cyber security
- o A strong understanding of the security requirements for online voting and the ability to relate these to appropriate security controls
- o Detailed knowledge of the NZISM (NZ Security Information Manual)

- o Knowledge of the CERT NZ Critical Controls 2018 and/ or other international information security frameworks (ISO 27000, NIST, CIS Security Controls).

Apologies if this sounds like a job description, but we are very aware of the importance of this, as I know you will be too.

Please get in touch to discuss the scope of the proposed role. We are very keen to have the government experts play some part in the process at this early stage, as security of the online voting system is a major focus and will have a major impact on public confidence in online voting as an option for future elections.

Kind regards

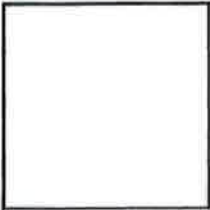
9(2)(a) (a)

[Redacted]

[Redacted]

[Redacted]

9(2)(a) [Redacted]



CAUTION: This email message and any attachments contain information that may be confidential and may be LEGALLY PRIVILEGED. If you are not the intended recipient, any use, disclosure or copying of this message or attachments is strictly prohibited. If you have received this email message in error please notify us immediately and erase all copies of the message and attachments. We do not accept responsibility for any viruses or similar carried with our email, or any effects our email may have on the recipient computer system or network. Any views expressed in this email may be those of the individual sender and may not necessarily reflect the views of Council.

Released under the Official Information Act 1982

OUT OF SCOPE

From: 9(2)(a) 9(2)(a)
Sent: Thursday, 13 September 2018 8:49 AM
To: 9(2)(a) <9(2)(a) a>
Subject: RE: Online voting - privacy commissioner - Reseller news

Hi 9(2)(a)

2 factor authentication is often mistaken for confirmation of identity, it isn't, it's a higher certainty that it's the same person returning, not ensuring the person is who they claim to be.

Government actually has an evidence of identity standard that DIA are custodians for if that's useful.

Cheers

9(2)(a)

From: 9(2)(a)
Sent: Wednesday, 12 September 2018 9:01 PM
To: 9(2)(a)
Subject: RE: Online voting - privacy commissioner - Reseller news

Yeah they will – 2 factor authentication. The councils are looking at pre-registration option.

9(2)(a) 9(2)(a) 9(2)(a)
Department of Internal Affairs | Te Tari Taiwhenua
9(2)(a) 9(2)(a) 9(2)(a) www.dia.govt.nz



Te Tari Taiwhenua
Internal Affairs

From: 9(2)(a)
Sent: Wednesday, 12 September 2018 1:00 PM
To: 9(2)(a)
Subject: FW: Online voting - privacy commissioner - Reseller news

Are you expecting in the regulations that you will address anything around the level of identity validation or verification?

They do so in the AML regulation I believe without specifying how, just a level of expectation.

From: [redacted]
Sent: Wednesday, 12 September 2018 12:47 PM
To: [redacted]
Cc: [redacted] [redacted] [redacted] [redacted]
Subject: Online voting privacy commissioner - Reseller news

Fyi.

https://www.reseller.co.nz/article/646586/privacy-commissioner-higher-standard-identity-verification-required-online-voting/?utm_campaign=channelbeat_pm-edition-2018-09-12&utm_source=channelbeat_pm-edition&utm_medium=newsletter&eid=486

[redacted] | [redacted]
The Department of Internal Affairs Te Tari Taiwhenua
45 Pipitea Street | PO Box 805, Wellington 6140, New Zealand | www.dia.govt.nz



COMMERCIAL IN CONFIDENCE.

Released under the Official Information Act 1982

9(2)(a)

9(2)(a)

From: 9(2)(a)

Sent: Thursday, 4 October 2018 11:02 AM

To: 9(2)(a) <9(2)(a) a>

Cc: 9(2)(a) !)(a) <9(2)(a) 2)(a)>

Subject: RE: Online voting - advice or contact for standards on secure operations

Hi 9(2)(a)

As discussed I think the answer to your question regarding the security etc. of the data is addressed by the classification that is given to the data and the retention / disposal would presumably be consistent with what the paper based is (i.e. time period etc).

Encryption is a step to address a security concern and links back in my mind to the classification.

I would re iterate my bigger concern is the linking of the individual to the vote itself, and the confidence that it is the right person voting, and while I understand the process is likely of no greater risk than the current off line process I am worried about the public perception on this and how it may be portrayed, and in turn what that might lead to in confidence in on-line voting full stop.

I've copied 9(2)(a) has been providing the technical advice on this engagement to date and I think is the most qualified of our team to help answer your questions.

9(2)(a) are you able to engage with 9(2)(a) on this to provide some guidance please, as I've noted above I don't think we are talking about creating a whole new set of requirements around on-line voting but if you have a different view on that lets get it on the table. Otherwise it might be providing some advice on where 9(2)(a) can confirm some of the details he needs.

Cheers

9(2)(a)

From: 9(2)(a)

Sent: Thursday, 4 October 2018 8:59 AM

To: 9(2)(a)

Subject: RE: Online voting - advice or contact for standards on secure operations

Importance: High

Hi 9(2)(a)

Further to the email below, I also need to speak to someone about another couple of aspects of online voting asap

We are looking to advice PCO in the coming days about:

- Content about security, custody, disposal of the online voting system and data.
- Whether levels of encryption should be specified in the exposure regulations.

Thanks

9(2)(a)

From: 9(2)(a)
Sent: Wednesday, 3 October 2018 4:25 PM
To: 9(2)(a)
Cc: 9(2)(a)
Subject: Online voting - advice or contact for standards on secure operations
Importance: High

Hi 9(2)(a)

As you may know, Policy are working on Local Electoral Online Voting Amendment Regulations. This to issue exposure regulations later this month.

We are hoping you can direct us to someone who can provide advice about standards for secure operation of online voting systems.

We anticipate the regulations will say something along the lines of the "the solution provider should provide evidence that the solution and operation of the solution have been tested and proven to meet appropriate standards for secure operation, such as ...".

SST's advice about potential standards to use in the regulations would be very useful.

We are operating to tight timeframes for these exposure regulations, so it would be great if you could get back to me shortly.

Thanks

9(2)(a) | 9(2)(a) | 9(2)(a)
The Department of Internal Affairs Te Tari Taiwhenua
Direct Dial: 9(2)(a)
45 Pipitea Street | PO Box 805, Wellington 6140, New Zealand | www.dia.govt.nz

INTERNAL AFFAIRS

Te Tari Taiwhenua

Requirements for a trial of online voting in local elections

A framework to guide Local
Government
November 2015

Released under the Official Information Act 1982



Contents

Purpose and status of this document	1
Introduction	2
How will local government demonstrate it is safe to proceed with a trial?.....	3
Why is the Government considering enabling a trial of online voting?	3
If a trial proceeds, which councils will take part?	5
Key principles for a trial of online voting	6
1. Functional requirements	8
Trial design	8
Online voting systems	9
2. Non-functional requirements	11
Usability and accessibility	11
Systems operation and process	11
Interoperability	14
Security	14
Audit system.....	17
Assurance and accountability	18
Appendix.....	20

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Purpose and status of this document

The Government is looking at enabling a limited number of territorial authorities to trial online voting in local elections in 2016. Territorial authorities would be responsible for procuring independently tested online voting services, and preparing for any trial.

This document provides the proposed operational outcomes for any trial of online voting in local elections. There will be further refinement of the framework to reflect engagement with stakeholders, testing of technology solutions, and amendments required in order to progress proposals for regulations. Additions, deletions and refinements adopted in relation to the framework will be advised as soon as possible to stakeholders, who will include councils, election service providers and developers of online voting services.

Regulations are required in order to authorise councils to participate in the trial, and to regulate its conduct. Participation by authorised councils will remain discretionary. The requirements of the Local Electoral Act 2001 and the final content of the framework, including information gathered from the testing and refinement of the framework, will inform the content of any regulations.

Released under the Official Information Act 1982

Introduction

In New Zealand, territorial authorities are responsible for the way elections are conducted in their area, including elections to regional councils, district health boards, local boards, community boards, and licensing trusts.¹ In practice, the actual running of local elections is now largely out-sourced. Presently, two New Zealand-based companies provide election services to nearly 90 per cent of local authorities.

The Local Electoral Act 2001 (the Act) and the Local Electoral Regulations 2001 together provide the framework for the running of local elections. Currently, under that framework, local authorities can carry out their elections by booth and/or postal voting. In practice, all authorities choose to solely use postal voting.² The Act anticipates other future voting methods and implementation of new technology. It specifies that "voting method" includes "any form of electronic voting"³, and allows new voting methods to be authorised by regulations.⁴

In recent years, a number of local authorities have asked for online voting to be allowed as a voting method for local elections. In light of this, in 2013, an Online Voting Working Party was established to consider the matter. The Working Party found that online voting has the potential to address some concerns with the current local electoral framework. However, there are significant risks associated with its use.⁵ The key risks relate to the security, accuracy, usability and availability of any technology solutions used for voting online. A lack of public confidence in online voting is also a risk to successful implementation and uptake. Further, technology failure as part of an online voting trial could undermine public confidence in local authority capability, any potential for future use of online voting by local government, and public comfort with carrying out other official transactions online.

A staged approach to any use of online voting is considered to be appropriate, as this allows all parties and stakeholders to become familiar with the opportunities and challenges presented by online voting.

What is online voting?

Online voting and e-voting are sometimes used interchangeably. Here, 'online voting' is used to refer to the form of voting where an elector is able to vote using the internet, remotely and unsupervised by officials, on the voter's own device. Use of the term online voting is not intended to include the use of electronic voting kiosks but may include use of publicly provided devices, such as computers in libraries.

¹ Local authorities are responsible for deciding the system of voting used (First Past the Post or Single Transferable Voting); deciding the method of voting used (postal voting, booth voting, or both); appointing electoral officials; and the conduct of local elections and polls, including the option of contracting companies to process and count votes.

² Booth voting was last used for local elections in 1992, by Hutt City Council.

³ Section 5 of the Local Electoral Act 2001.

⁴ Section 139 of the Local Electoral Act 2001.

⁵ Retrieved 29 October 2014, from [http://www.dia.govt.nz/pubforms.nsf/URL/Online-Voting-in-New-Zealand-report.pdf/\\$file/Online-Voting-in-New-Zealand-report.pdf](http://www.dia.govt.nz/pubforms.nsf/URL/Online-Voting-in-New-Zealand-report.pdf/$file/Online-Voting-in-New-Zealand-report.pdf).

In December 2014, the Government decided that while it did not have an objection in principle to local government trialling online voting, such a trial would not be allowed to proceed until local government had demonstrated that voting technology solutions can be used in a way that meets the requirements of the Act and security expectations.

How will local government demonstrate it is safe to proceed with a trial?

Territorial authorities trialling online voting in their area will be responsible for demonstrating that voting technology solutions can be used in a way that meets the requirements of the Act and security expectations. They will demonstrate this by obtaining independent assurance that the technical specifications for voting technology solutions to be used in their elections meet the Government's requirements contained in this document. They will also obtain independent assurance that the voting technology solution itself is in compliance with the technical specifications that the territorial authority or their election service provider have prepared.

Why is the Government considering enabling a trial of online voting?

Ensuring fair, effective and efficient electoral processes and procedures, for voters and candidates, is a necessary pre-requisite for healthy and vibrant democratic practice. The combination of a highly IT-enabled population⁶ and dissatisfaction among some electors with the current voting experience has prompted many local authorities to seek to trial online voting. Some of the ways online voting has the potential to improve future local authority elections are discussed.

Enhancing accessibility

Online voting has the potential to assist certain groups of electors who currently have issues exercising their right to vote under the postal system. These include those who are living in remote areas or overseas at election time, and those who (because of disability or language issues) cannot vote unassisted.

There are reported instances where those living in remote areas or overseas at election time have not received their documents in time to vote. In the 2013 local elections, about five percent of overseas electors who were issued a voting pack actually voted, which is significantly lower than the average voter turnout of 41 percent. This suggests that voters overseas may find postal voting limits opportunities to vote. Online voting may make it easier for those that wish to vote overseas. It may also assist those living in remote areas with limited postal services.

⁶ The World Internet Project 2013 puts New Zealand's penetration of the internet at 92 per cent. *Online voting in New Zealand: feasibility and options for local elections – Report of the Online Voting Working Party*, page 12. Retrieved 29 October 2014, from [http://www.dia.govt.nz/pubforms.nsf/URL/Online-Voting-in-New-Zealand-report.pdf/\\$file/Online-Voting-in-New-Zealand-report.pdf](http://www.dia.govt.nz/pubforms.nsf/URL/Online-Voting-in-New-Zealand-report.pdf/$file/Online-Voting-in-New-Zealand-report.pdf).

Some electors who struggle with postal voting could find it easier to vote. Electors that are visually-impaired,⁷ have low proficiency in literacy,⁸ or for other reasons may need assistance to fill out their voting documents. Finding assistance can be difficult and, once a voter finds assistance, they are unable to vote in secret. Online voting could allow these groups to be able to vote more easily and privately..

Improving accuracy

Online voting provides opportunities to make the act of voting simpler and more accurate, by notifying voters if they have incorrectly completed a voting document. Under the current postal voting system, inaccuracy can arise where voters submit a voting document that does not properly record their intent. Voters are not notified that their vote qualifies as informal, and there is no formal verification system for people to check how their vote is counted.

Due to the use of the Single Transferable Voting (STV) and the First Past the Post (FPP) systems of voting, voting in local elections can be complex, resulting in greater potential for voter-error. For the 2013 local authority elections, the number of blank and informal votes ranged from 0.4 – 13.9 per cent of the total votes per local authority. For district health board elections (which are all run as STV elections), this number ranged from 9.5 – 22.4 per cent. Although some of these may have been deliberately spoiled voting documents, there are also voters who accidentally spoil their voting document, such as by giving multiple candidates the same ranking in an STV election.

Local election modernisation

New Zealanders conduct many of their activities online and also have a number of devices to access the internet.⁹ There is growing public expectation that online voting will become available soon, in line with the many other activities already undertaken online. Being able to offer online voting aligns with broader commitments of some local authorities to service modernisation, efficiency and 'going digital'.

Cost and frequency of postal services

The current reliance on postal voting also presents some potential risks to the viability of local elections in the longer term. Declining use of postal mail and the shift towards digital communication both reflect and reinforce the changing preferences of New Zealanders for how they communicate and conduct their affairs, which links back to matters of accessibility.

⁷ According to Statistics New Zealand, in 2013, 168,000 people had varying issues with seeing, many of whom could have required assistance to vote. Statistics New Zealand. *The New Zealand Disability Survey 2013*. Wellington: Statistics New Zealand, 2014. http://www.stats.govt.nz/browse_for_stats/health/disabilities/other-versions-disability-survey_2013.aspx [accessed 17 February 2015].

⁸ According to the Ministry of Education, 87 percent of New Zealanders achieved above the lowest proficiency for prose literacy. This means 13 percent achieved the lowest level of proficiency in prose literacy. Available at: <http://www.educationcounts.govt.nz/indicators/main/education-and-learning-outcomes/26327> [accessed 18 February 2015].

⁹ In 2012, 2.8 million New Zealanders connected to the internet, with 90 percent of 15 to 44 years olds being connected. Statistics New Zealand. *New Zealanders' connection with the Internet*. Available at: http://www.stats.govt.nz/browse_for_stats/snapshots-of-nz/yearbook/people/population/7-million.aspx [accessed 19 February 2015].

The current legislative framework for local elections does not offer sufficient flexibility to start shifting away from a paper-based system, thus preventing local decision-making around what may be appropriate for engagement with the local community.

Select Committee support

The Justice and Electoral Committee indicated support for trialling online voting in its inquiries into the 2010 and 2013 local elections.

If a trial proceeds, which councils will take part?

There is no obligation on councils to participate in a trial. The Associate Minister of Local Government is seeking from Local Government New Zealand (LGNZ), confirmation of which territorial authorities believe they can meet the requirements in this document and wish to proceed with a trial of online voting. The Minister will also seek LGNZ's view on the appropriate size for a trial to ensure that any trial will produce evidence of the practicality and value of online voting in local elections across New Zealand. A decision on this will need to be made before the regulations to enable a trial are to be made, at the end of 2015.

Released under the Official Information Act 1982

Key principles for a trial of online voting

The Local Electoral Act has three core principles underpinning it:

- fair and effective representation for individuals and for communities
- all qualified people have a reasonable and equal opportunity to cast an informed vote to nominate a candidate and to become a candidate
- public confidence in local electoral processes and public understanding of local electoral processes including: protection of the freedom of choice of voters and the secrecy of the vote, transparent electoral systems and voting methods and certainty in electoral outcomes.

These core principles have implications for the way a trial of online voting must work. More specific principles that represent the application of the core principles to a trial of online voting are discussed below. These in turn underpin the policy requirements set out further in this document.

Equivalence with current system

The concept of people having reasonable and equal opportunity to vote supports electors having options as to *how* they vote. As such, in an online voting trial, it is important that online voting is only made available to electors as an additional option to postal voting. Further to this, the principles of equality of opportunity to vote and retaining public confidence require that the rules and requirements for online voting are generally equivalent to those for postal voting i.e. are similar except where features of online voting require different provisions to achieve the same or an equivalent outcome. For example:

- Voter coercion has a similar risk profile under both postal and online voting, as in both cases voting is unsupervised by officials and so more stringent protections are not required in the online voting context; but
- Security risks associated with the interception and manipulation of votes once they leave the voter are greater for online voting than postal voting; therefore higher as well as different sorts of requirements will need to apply to online voting.

The principle of equivalence is also important where some elections (e.g. for regional councils or district health boards) are conducted partly in territorial authorities using online voting and partly where this is not the case.

Secrecy of the vote/voter privacy

Further steps need to be considered to ensure that secrecy of the vote is adequately protected, in light of new risks presented by use of the internet. However, it is acknowledged that there are limited means by which an online voting system can influence whether a secure environment exists. It is also important that security requirements do not detract from the provision of a reasonable opportunity to vote that preserves equivalence with postal voting.

Transparency/verifiability

It is particularly important, given the “invisible” nature of online voting processes and opportunities for tampering with these, that the transparency of the online voting system is demonstrated through audit processes that verify accuracy of the system. Such additional requirements are important for ensuring equivalence of public confidence in election results with those conducted using postal voting.

Local government accountability

The way online voting trials are conducted needs to support the role and accountability of electoral officers under the local electoral framework. At the same time, the territorial authorities that choose to participate in a trial accept responsibility for ensuring there is adequate resourcing for an online voting trial in their area, that they meet security expectations, and that they will maintain the integrity of local elections practice. This is consistent with the concept of local government responsibility for local elections that underlies in the local electoral regulatory framework.

Development of requirement for a trial of online voting

Many of the requirements contained in this document have been developed from the Council of Europe Recommendation *Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*.¹⁰ While derived from that recommendation, those requirements have been adapted for the New Zealand local electoral context. A table of cross-references is provided in the appendix to this document, to assist in the understanding of the development of such requirements.

Requirements contained in the Council of Europe recommendation have formed guidance for online voting systems in many countries. Independent assessments of how these systems achieved compliance with those requirements can inform useful discussion. One such example is an assessment report by the International Foundation for Electoral Systems on the Norwegian E-vote Project.¹¹

Matters not anticipated by this document

Where a matter arises for which there is not a requirement in this document, the principle of equivalence with the current postal voting system should be applied.

¹⁰ This recommendation is available on the Council of Europe’s website. Retrieved 16 April 2015, from http://www.coe.int/t/DEMOCRACY/ELECTORAL-ASSISTANCE/themes/evoting/default_en.asp.

¹¹ Retrieved 16 April 2015, from https://www.regjeringen.no/globalassets/upload/krd/prosjekter/e-valg/evaluering/topic7_assessment.pdf.

1. Functional requirements

This section covers how online voting should work, and how any online voting system should operate. Note that in this document, use of the term 'online voting system' refers to all components that work together to enable an elector to vote online. This includes systems used at the pre-voting stage, such as to generate or hold voter-related information. It includes the core technology solution that provides an internet-based voting platform, electronically stores votes received online, and enables voters to verify their vote. It also includes systems used at the post-voting stage, such as counting software, which may already be in use under the postal voting system. References to 'relevant electoral officer' mean the electoral officer for the relevant territorial authority participating in a trial.

Trial design

- 1.1 Online voting must only be made available as an additional option alongside postal voting.
- 1.2 Voters must be able to vote online using their own internet-capable device, and without any need to install additional software (excluding any required browser upgrades).
- 1.3 Territorial authorities must explicitly define the availability requirements for their online voting system. In doing so they should take into account voter needs, community expectations and how many of their voters may be seeking to vote online from different time zones.
- 1.4 Electors must be able to vote online without being required to pre-register.
- 1.5 Voters must be informed, well in advance of the start of voting, of the way in which online voting will be organised, and any steps a voter may have to take in order to participate and vote.
- 1.6 Online voters must be able to access online, the same degree of information about candidates as postal voters do with hard-copy documents.
- 1.7 The period in which an electronic vote can be cast must be:
 - 1.7.1 defined and made known to the public well in advance of the start of voting, and
 - 1.7.2 the same as the time allowed for receipt of postal votes, subject to requirement 2.13.
- 1.8 User experience feedback must be enabled and collected to feed into overall trial learnings.
- 1.9 All electors in an election for which online voting is being used must be provided with an opportunity to find out if an online vote has been received and recorded under their name, and must be notified of this opportunity. This opportunity must be provided separately from the casting of a vote online, and provided regardless of whether and how an elector chooses to vote. Online voters must be provided with an opportunity to opt in to receive an email notification that an online vote has been received and recorded under their name. To facilitate this, there must be an ability to supply an email address after casting an online vote.

Online voting systems

- 1.10 Before casting a vote online, voters' attention must be explicitly drawn to the fact that the election in which they are submitting their electronic vote is a real election. If opportunities to practice online voting are offered, participants must have their attention drawn explicitly to the fact that they are not participating in a real election and must, when practice opportunities are continued at election times, at the same time be invited to cast their vote in the real election.
- 1.11 A valid voter ID and access code, enabling an elector to authenticate him or herself online, must be transmitted to electors independently of each other in separate transactions.
- 1.12 All voting options, and any information about voting options accessible from the online voting site, must be presented in an equal, unbiased manner.
- 1.13 The way in which voters are guided through the online voting process must discourage their voting without proper opportunity for reflection.
- 1.14 Voters must be able to alter their choice at any point in the online voting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person.
- 1.15 If the vote capture device requires a response by a voter within a specific period of time, it must provide fair warning, by issuing an alert a reasonable time before this time period has expired and provide a means by which the voter may receive additional time.
- 1.16 Before submission of a vote, the online voting technology solution must require a voter to confirm their selection and intention to cast the vote.
- 1.17 The online voting system must provide the voter with an opportunity to deliberately submit a blank or incomplete voting document.
- 1.18 Where an online voting document has been incorrectly marked, the online voting technology solution must inform the voter of the nature of the error that has been made and give them an opportunity to fix the error before submission of the voting document.
- 1.19 The online voting system must indicate clearly to the voter when the vote has been submitted successfully and the voting procedure has been completed.
- 1.20 The voter must be informed about the means to verify that a connection to the official server has been established and that the voting document presented is genuine.
- 1.21 The voter must be informed of how to delete, where that is possible, traces of the vote from the device used to cast the vote.
- 1.22 The online voting system must not allow a voter to submit more than one vote for any election.
- 1.23 The online voting system must prevent the changing of a vote once that vote has been cast.
- 1.24 The online voting system must not enable the voter to be in possession of a proof of the content of the vote cast.
- 1.25 Immediately after their votes have been submitted, voters must be provided with a separate opportunity to submit feedback on their experience.

- 1.26 Online voting must be designed in a way that protects the secrecy of the vote at all stages of the voting process.**
- 1.27 The design of the online voting system must guarantee that votes submitted online are, and will remain, anonymous.**
- 1.28 The online voting system must be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.**
- 1.29 The online voting system must prevent processing information on submitted votes that could reveal individual voters' choices.**

Released under the Official Information Act 1982

2. Non-functional requirements

This section covers requirements to ensure online voting works well.

Usability and accessibility

- 2.1 The voter interface of an online voting technology solution must be understandable and easy to use.
- 2.2 Online voting systems must be designed, as far as it is practicable, to maximise the opportunities that such systems can provide for persons with disabilities.
- 2.3 Users and/or representative user organisations must be involved in the design of online voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.
- 2.4 Online voting technology solutions must support and be tested in any browser or device used by more than 1 percent of people accessing sites of the territorial authority in question.
- 2.5 The voter interface must conform at Level AA to the W3C's Web Content Accessibility Guidelines (WCAG) 2.0.
- 2.6 Usability and accessibility measures should not detract from the secrecy and integrity of the election.

Systems operation and process

- 2.7 Online voting systems and processes must preserve the integrity of individual votes and local elections as a whole, and the online voting process must be verifiable end-to-end.
- 2.8 The authenticity, availability and integrity of all election data must be maintained.
- 2.9 Measures must be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.
- 2.10 Decrypting required for the counting of the votes must not be carried out until the voting period has closed.
- 2.11 No invalid (informal or out of time) votes must enter the electronic ballot box
- 2.12 In the last hour of voting at least, the voter interface must inform an elector of the time remaining before close of voting.
- 2.13 The online voting system must allow voters who are logged on when the voting period ends, to complete and submit their votes during a grace period not exceeding five minutes after the close of voting.
- 2.14 Those responsible for operating the equipment must draw up a contingency procedure. Any backup system must conform to the same standards and requirements as the original system.
- 2.15 Sufficient backup arrangements must be in place and be available throughout the voting period to ensure that voting proceeds smoothly. Appropriately authorised persons concerned must be ready to intervene rapidly according to a procedure drawn up by the relevant electoral officer.

- 2.16 Immediately before the election, the equipment must be checked and approved in accordance with a protocol drawn up by the relevant electoral officer. The equipment must be checked to ensure that it complies with technical specifications. The findings must be submitted to the relevant electoral officer.
- 2.17 All technical operations must be carried out in accordance with an agreed procedure for controlling operations in the online voting system. Any substantial changes to key equipment must be authorised by the relevant electoral officer.
- 2.18 Key election equipment, such as servers, must be located in a secure area and that area must, throughout the election period, be guarded against interference of any sort and from any person.
- 2.19 A disaster recovery plan must be in place during the election period.
- 2.20 Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment must immediately inform the relevant electoral officer, who will take the necessary steps to mitigate the effects of the incident. The level of incident which must be reported must be specified in advance by the relevant electoral officer.
- 2.21 In the event of any irregularity affecting the integrity of votes, the affected votes must be recorded as such.
- 2.22 Except to allow overseas voters the ability to vote online, vote and voter related information must not be transmitted or held outside New Zealand at any point before, during, or after an election.
- 2.23 Information on the functioning of an online voting system must be made publicly available.
- 2.24 Critical election configuration and management processes must require the participation of teams of more than one appropriately authorised person (two-eyes principle). As far as possible, such activities must be carried out outside the election period.
- 2.25 The online voting system must be accessible only to persons who are eligible to vote. The online voting system must require authentication of the elector and must ensure that the elector is enabled to vote in all elections for which the elector is qualified and no other election.
- 2.26 After the end of the voting period, no voter must be allowed to gain access to the voting platform.
- 2.27 The online voting system must contain measures to preserve the availability of its services during the voting process. It must resist, in particular, malfunction, breakdowns or denial of service attacks, according to the specifications of the territorial authority taking part in the trial of online voting.
- 2.28 While an electronic ballot box is open, any authorised intervention affecting the online voting technology solutions must be carried out by teams of at least two people, be the subject of a report, and be monitored by representatives of the relevant electoral officer.
- 2.29 The online voting system must maintain the availability and integrity of the votes. It must also maintain the confidentiality of the votes and keep them sealed until the counting process, except as required to give effect to requirement 2.43. If stored or communicated outside controlled environments, the votes must be encrypted.

- 2.30 Technical and organisational measures must be taken to ensure that no data will be permanently lost in the event of a breakdown or a fault affecting the online voting system.
- 2.31 The online voting system must maintain the privacy of individual voters, protecting the secrecy of the vote and maintaining, until the close of voting, the confidentiality of the names of persons from whom voting documents have been received.
- 2.32 The online voting system must perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available.
- 2.33 The online voting system must restrict access to its services, depending on the user identity or the user role, to those services explicitly assigned to this user or role. User authentication must be effective before any action can be carried out.
- 2.34 Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) must be ensured.
- 2.35 Online voting systems must generate reliable and sufficiently detailed data so that election observation can be carried out.
- 2.36 The online voting system must maintain reliable synchronised time sources. The accuracy of the time source must be sufficient to maintain time marks for audit trails and observations data, as well as for maintaining the time limits for voting.
- 2.37 The online voting system must be able to ascertain that a vote has been cast within the prescribed time limits.
- 2.38 The online voting system must ensure that the voter's choice is accurately represented in the voting document and that the submitted voting document is securely recorded.
- 2.40 The integrity of data communicated during the voting stage (e.g. votes, lists of candidates) must be maintained. Data-origin authentication must be carried out.
- 2.41 The online voting system must maintain the availability and integrity of the electronic ballot box as long as required.
- 2.42 Voter surveys and their final reports must not compromise directly or indirectly (statistically or by linking information) the secrecy of the vote.
- 2.43 The relevant electoral officer must enable the voter to individually verify that his/her vote is recorded as intended at any time between the commencement of voting and the deadline for filing a petition for inquiry into the conduct of the relevant election. Verification must be in person and subject to the electoral officer's satisfaction as to the voter's identity. The electoral officer must keep a record of all individuals who verify their vote, whether their vote is recorded as it should be, and any election that is affected in the event that there is a discrepancy.
- 2.44 The online voting system must allow for an observer or independent auditor to verify that votes are counted as recorded.
- 2.45 The end to-end verifiability measures must not compromise the secrecy of the vote.

Interoperability

Between online systems

- 2.46 All components of the online voting system must be interoperable.
- 2.47 The online voting system must use open standards and protocols to ensure that the various technical components or services of an online voting system are interoperable with the applicable counting and other local electoral systems.
- 2.48 A procedure must be established for regularly installing updated versions and corrections of the relevant protection software. It must be possible to check the state of protection of the voting equipment at any time.
- 2.49 An online voting technology solution must prove its successful interoperability with counting and other local electoral systems by undertaking a test and documenting the results.

With postal voting system

- 2.50 There must be a secure and reliable method to aggregate electronic and postal votes and to calculate the correct result.
- 2.51 Aggregated votes must be counted using the counting processes under the existing postal voting system.
- 2.52 The design of an online voting technology solution must allow for votes to be able to be removed from the electronic ballot box following the processing of special votes.

Security

- 2.53 Online voting systems must be secure and reliable.
- 2.54 Online voting systems must comply with New Zealand Government standards and industry best practice for web and applications security, including, at a minimum: the New Zealand Information Security Manual (NZISM), ISO27001, ISO27002 and the OWASP Top 10; and should also meet other web security standards such as the ASD Top 35 mitigations and then SANS Top 25.
- 2.55 Any online voting system must comply with all mandatory requirements in the NZISM, for government departments regarding security standards for data classified as "In Confidence".
- 2.56 Territorial authorities taking part in an online voting trial must assess the broader security risks through the Protective Security Requirements Framework.

Procurement and service provider selection

- 2.57 Territorial authorities taking part in an online voting trial must employ appropriately skilled personnel to assist with implementation and running of the trial.
- 2.58 Where a territorial authority does not have appropriately skilled staff, an approved assurance provider (from the public service's ICT Security and Related Services Panel) should be engaged to validate the level of security applied to the online voting system.¹²
- 2.59 Where territorial authorities seek to use a cloud computing service as a part of participating in an online voting trial, territorial authorities must follow the Government Chief Information Officer's Requirements for Cloud Computing guidance where the online voting system uses a cloud-based service, including endorsement of the solution and acceptance of the residual risks by the head of the territorial authority.¹³ In order to inform the solution/tender selection process for cloud-based solutions, territorial authorities must complete the information risk assessment using the All-of-Government 'Cloud Security and Privacy Considerations' questionnaire prior to commencing final contracting negotiations.
- 2.60 All resulting assurance documentation (endorsement and supporting cloud risk assessment) must be submitted to the Government Chief Information Officer for assurance endorsement purposes.

Risk assessment, assurance, and certification and accreditation

- 2.61 Territorial authorities taking part in an online voting trial must perform a risk assessment prior to selecting a service provider, in line with the Government Chief Information Officer's All-of-Government information security risk assessment process.¹⁴
- 2.62 Any online voting system that is to be selected must be:
- 2.62.1 assessed to determine its level of security;
 - 2.62.2 certified and accredited through a standardised process, with, at a minimum, the following steps:
 - 2.62.2.1 Risk assessment (RA) – understanding the business and technical context of the information system and identifying the relevant security risks;
 - 2.62.2.2 Privacy Impact Assessment (PIA) – understanding the privacy context and value of the information held in the system;
 - 2.62.2.3 Penetration testing (PT) – to test for vulnerabilities in the system;
 - 2.62.2.4 Statement of applicability (SoA) – identifying the applicable security controls based off leading standard
 - 2.62.2.5 Controls validation plan (CVP) – identifying the documentation and evidence needed to validate the security controls identified in the SoA;

¹² <https://www.ict.govt.nz/services/show/SRS-Panel>.

¹³ <https://www.ict.govt.nz/guidance-and-resources/information-management/requirements-for-cloud-computing/>.

¹⁴ <https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf>.

2.62.2.6 Controls validation audit (CVA) – using the CVP to audit the relevant security controls;

2.62.2.7 Certification – assessing the completeness and effectiveness of the security controls that were audited; and

2.62.2.8 Accreditation – granting authority to operate the information system.

Technical assessment and testing of the online voting system prior to use

2.63 Territorial authorities must use an approved provider from the public service's ICT Security and Related Service Panel to undertake all security testing, assessment, and certification and accreditation.

2.64 Territorial authorities must undertake appropriate remediation activities following penetration testing and prior to the online voting system being used.

2.65 Additionally, territorial authorities should conduct:

2.65.1 a further penetration test, using a different Panel provider, prior to the system being used in an election; and

2.65.2 a 'red team' exercise to test the service providers' and authorities' security management and incident response capabilities.

Incident detection, response and management

2.66 A service providers' incident detection capability must be considered as a part of the procurement process.

2.67 A service providers' incident response capability must be considered as a part of the procurement process.

2.68 Any service provider selected to operate an online voting system should have their incident management capability and processes validated during the certification and accreditation process.

Security education and awareness

2.69 Territorial authorities should create and disseminate awareness material to educate voters about device security and what steps they can take to improve the security of their devices before they use the online voting system.

2.70 Territorial authorities should consider providing secure facilities to allow voters to access the online voting system and cast their votes.

2.71 Territorial authority business and technology teams undertaking a trial of online voting should establish connections with international counterparts who have successfully implemented online voting systems.

Confidentiality

2.72 Votes and voter information must remain sealed as long as the data is held in a manner where they can be associated. Authentication information must be separated from the voter's decision at a pre-defined stage in the election.

- 2.73 The online voting system must protect authentication data so that unauthorised entities cannot misuse, intercept, modify, or otherwise gain knowledge of all or some of this data.

Integrity

- 2.74 Territorial authorities must put in place all appropriate and reasonable security controls to avoid the possibility of fraud or unauthorised intervention affecting the system during the whole voting process.
- 2.75 Sufficient means must be provided to ensure that the system used by the voters to cast the vote can be protected against influence that could modify the vote.

Availability

- 2.76 Territorial authorities, or their services providers, must have measures to ensure availability, within defined requirements, in place, and audited, as a part of the certification and accreditation process.

Audit system

- 2.77 The online voting system must be auditable end-to-end.
- 2.78 The audit system must be designed and implemented as part of the online voting system. Audit facilities must be present on different levels of the system: logical, technical and application.
- 2.79 End-to-end auditing of an online voting system must include recording, providing monitoring facilities and providing verification facilities.
- 2.80 The audit system must be open and comprehensive, and actively report on potential issues and threats.
- 2.81 The audit system must record times, events and actions, including:
- 2.81.1 all voting-related information, including the number of eligible voters, the number of votes cast, the number of invalid votes, the counts and recounts, etc.;
 - 2.81.2 any attacks on the operation of the online voting system and its communications infrastructure;
 - 2.81.3 system failures, malfunctions and other threats to the system.
- 2.82 The audit system must provide the ability to oversee the election and to verify that the results and procedures are in accordance with the applicable policy, procedural and legal requirements.
- 2.83 Disclosure of the audit information to unauthorised persons must be prevented.
- 2.84 The audit system must maintain voter anonymity at all times.
- 2.85 The audit system must provide the ability to cross-check and verify the correct operation of the online voting system and the accuracy of the result, to detect voter fraud and to prove that all counted votes are authentic and that all votes have been counted.

- 2.86 The audit system must be protected against attacks which may corrupt, alter or lose records in the audit system.
- 2.87 The conclusions drawn from the audit process must be documented to ensure that the election is true and accurate and to feed into overall trial learnings.

Assurance and accountability

Territorial authorities

- 2.88 Territorial authorities must have in place, a project governance structure to:
- Ensure that the design of the online voting as a service is underpinned by a comprehensive assessment of the risks involved in the successful completion of the particular election. The online voting system must include the appropriate safeguards, based on this risk assessment, to manage the specific risks identified.
 - Ensure service failure or service degradation are kept within pre-defined limits.
 - Ensure that voters understand and have confidence in the online voting system, and that electors are made aware that all rights and responsibilities existing under the Local Electoral Act 2001 still apply in the online voting context.
 - Advise the Chief Executive of the territorial authority in question whether online voting is safe to proceed prior to its use in an election.
- 2.89 Territorial authorities have overall responsibility for ensuring compliance with these policy requirements. Territorial authorities must also undertake project assurance of the development of online voting systems and services.
- 2.90 Territorial authorities must appoint an independent assurance provider to provide an impartial and independent assessment of the matters in 2.88. The appointment of the independent assurance provider must be approved by the Secretary for Local Government.
- 2.91 Before any online voting system is used in an election, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent assurance provider appointed by the relevant territorial authority must, in the prescribed manner, verify that the online voting system is working correctly and that all the necessary security measures have been taken.
- 2.92 Before any online voting system is used in an election, the Chief Executive of the territorial authority in question must advise the Secretary for Local Government in writing that:
- he or she considers that all relevant risks have been identified and mitigated to the extent that it is considered safe to proceed with use of online voting, confirming that the relevant electoral officer is of the same opinion.
 - The territorial authority has sought and received endorsement of project assurance from the Government Chief Information Officer.
- 2.93 Territorial authorities must provide to the Secretary for Local Government, copies of all assessments and other documentation necessary to enable a full independent assessment of their online voting systems and services.

Electoral officers

- 2.94** The electoral officer for a territorial authority conducting an online voting election must be cognisant of all components of the online voting system, as required for verification and certification purposes.
- 2.95** Before any online voting election takes place, the electoral officer must be satisfied that the online voting system is legitimate and operates in accordance with these requirements and relevant legislation.
- 2.96** The electoral officer must ensure that only persons authorised by the electoral officer have access to the central infrastructure, the servers and the election data. There must be clear rules established for such authorisation, and all such persons must be subject to sections 14 and 131 of the Local Electoral Act 2001.

Released under the Official Information Act 1982

Appendix

This Appendix is only included to assist in the understanding of the development of policy requirements contained in this document. It cross-references the requirements contained in this document with similar requirements contained in the Council of Europe (CoE) Recommendation *Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*. More information on the relevance of those requirements is provided on page 7 of this document.

Requirement no. (NZ)	Requirement no. (CoE)	Requirement no. (NZ)	Requirement no. (CoE)	Requirement no. (NZ)	Requirement no. (CoE)
1.1	4	2.14	70	2.56	
1.2		2.15	71	2.57	
1.3		2.16	73	2.58	
1.4		2.17	74	2.59	
1.5	38	2.18	75	2.60	
1.6		2.19	75	2.61	
1.7	37	2.20	76	2.62	
1.8		2.21	58	2.63	
1.9		2.22		2.64	
1.10	50	2.23	21	2.65	
1.11		2.24	32	2.66	
1.12	12, 47, 49	2.25	94	2.67	
1.13	10	2.26	96	2.68	
1.14	11	2.27	30	2.69	
1.15		2.28	33	2.70	
1.16		2.29		2.71	
1.17	13	2.30	77	2.72	35
1.18		2.31	78	2.73	81
1.19	14	2.32	79	2.74	29
1.20	90	2.33	80	2.75	92
1.21	93	2.34	82	2.76	
1.22	5	2.35		2.77	59
1.23	15	2.36	84	2.78	100
1.24	51	2.37	91	2.79	101
1.25		2.38	95	2.80	102
1.26	16	2.39	96	2.81	103
1.27	17	2.40	97	2.82	104
1.28	18	2.41	99	2.83	105
1.29	54	2.42		2.84	106
2.1	1	2.43		2.85	107
2.2	3	2.44		2.86	109
2.3	62	2.45		2.87	60
2.4		2.46		2.88	
2.5		2.47		2.89	85
2.6		2.48	69	2.90	85
2.7	26	2.49		2.91	25
2.8	83	2.50		2.92	
2.9	19	2.51		2.93	
2.10	55	2.52		2.94	24
2.11		2.53	28	2.95	31
2.12		2.54		2.96	
2.13		2.55			