NSW Electoral Commission
Technology Assisted Voting

Initiation brief for the
iVote Refresh Project

Issued 17 November 2017

New South Wales Electoral Commission
ABN. 94 828 824 124

Level 25
201 Kent Street Sydney NSW 2000
GPO Box 832, Sydney NSW 2001

Contents

1. Introduction

1.1 Context of this document

The New South Wales Electoral Commission (NSWEC) has previously published a range of data and documents about the iVote® system[1] which enables people to vote online or by phone.

The NSWEC has begun a new project to implement updates and improvements to iVote for use at the 2019 NSW State General Election (the "iVote Refresh Project").

To ensure ongoing transparency of the iVote Refresh Project, this document explains some key factors the NSWEC will consider as it develops the strategy for the new iVote.

The NSWEC's iVote Strategy, to be published by mid-2018, will:

- build upon the *iVote Strategy for the NSW State General Election 2015*
- outline longer-term goals for the use of iVote
- place the new version of the iVote system within the context of those goals.

The 2018 Strategy will provide a detailed overview of the new electronic voting system and how it is intended to be used at the March 2019 NSW State General Election.

This document is intended to provide an insight into the NSWEC's current high-level thinking about elements of the iVote Refresh Project and proposed 2018 Strategy, having regard to what we have learned through our engagement with internet voting technology suppliers and an examination of academic research.

1.2 Transparency

The NSWEC's aim is to be as transparent as possible as it rolls out this project. With this in mind, we have identified three key ways in which the use of iVote can be made transparent:

- Publishing information about the design and implementation of the technology components and processes.
- Enabling meaningful observation of the operation of iVote during election events.
- Publishing data about an election event, both during and after the event.

What we can make available will depend on the design and specifications of the system that is eventually procured for the iVote Refresh Project.

[1] iVote is a registered trademark of the NSW Electoral Commission. However, the registration symbol will not be used throughout the rest of this document.

2. Background

The NSWEC is the statutory body that manages elections in New South Wales. Following an amendment in 2010 to the *Parliamentary Electorates and Elections Act 1912* to enable the use of 'technology assisted voting', the NSWEC developed iVote and has offered it at:

- the 2011 and 2015 NSW State General Elections
- nine NSW State By-elections
- the March 2017 Western Australian State General Election.

The iVote System allows eligible people to cast their votes by telephone or by computer using the internet. Under the legislation, this includes voters who:

- are blind or have low vision
- are illiterate or have other disabilities
- live more than 20km from a polling place
- will be interstate or overseas on an election day.

In 2016 the iVote system won the Australian Government's *Excellence in eGovernment – Service Delivery* Award. The NSWEC was also a finalist for iVote in the *Service transformation for the digital consumer – Government* category of the Australian Computer Society's 2016 Digital Disruptors Awards.

2.1 The iVote refresh project

Internet voting is an area of technology that is developing rapidly. While the current iVote system has successfully delivered a number of NSW election events, the NSWEC is seeking to procure an enhanced version for use at the 2019 NSW State General Election. The primary objectives are to:

1. Enhance system security and voting protocol integrity by:
    - improving the voting protocol in regards to verification (both voter verification and universal verification)
    - updating cyber-security across the platform.
2. Increase transparency, auditability and scrutiny (including scrutiny by candidates and parties).
3. Enhance functionalities and user experience which includes:
    - allowing the system to support more than one election at a time; and
    - introducing support for some community languages to the web interfaces.
4. Enhance public awareness of iVote with targeted promotion to community and disability groups.

The NSWEC's decision to undertake this procurement process should not be seen as indicating dissatisfaction with the current Scytl Core Voting System.

As noted in the *iVote Refresh Program Procurement Strategy* document, published in May 2017, the NSWEC is confident that the organisations named in that document (including Scytl) would have the capability to deliver and support such an enhanced voting system.

Having said this, there are currently no suitable suppliers on NSW government procurement panels and, to meet the NSW Government's procurement requirement, the NSWEC is undertaking an open tendering process.

2.2 Strategic context for the NSWEC

The *NSWEC Strategic Plan 2017-20* articulates our vision to "maintain confidence in the integrity of the democratic process and make it easy for people to understand and participate."

Technology assisted voting, with the iVote system, is a key element in achieving this vision. The iVote Refresh Project particularly supports our two outward-looking strategic goals:

1. Customer focused products and services that deliver seamless end-to-end electoral services.
2. Engagement, influence and advocacy to build reach, impact, influence and collaboration with our key stakeholders to improve our engagement and delivery.

The iVote Refresh is primarily captured within the strategy's objective 1.2: "*Make all our services easy to use and secure, by leveraging opportunities from new technology,*" which has two initiatives:

- online tools and services
- election innovations

It is also linked to initiatives under strategies 2.1 ("*Build brand and customer engagement*") and in particular 2.2 ("*Improve voter participation through easy communications and better, user centred digital services*"). The iVote Project also aligns with the NSWEC's customer-centred design principles.

2.3 iVote inquiry

While NSWEC has commenced the iVote Refresh Project to deliver a new version of the iVote system for 2019, it should be noted that, in response to a recommendation of the NSW Parliament's Joint Standing Committee on Electoral Matters, the NSWEC has initiated an inquiry into iVote to examine the current iVote system. Public submissions close on 31 December 2017 and the report is anticipated to be delivered in May 2018.

The iVote inquiry website contains more information about the terms of reference.

3. Principles

NSWEC is actively working on the development of guiding principles for electronic voting, including reviewing international standards and working with other Australian electoral commissions.

At a meeting of the Electoral Council of Australia and New Zealand (the ECANZ) on 4 July 2017, all Australian electoral commissions endorsed 11 essential principles for an internet voting service. These principles reflect existing best electoral practices as they apply to current voting channels.

The ECANZ examined the United States Election Assistance Commission's 'Voluntary Voting System Guidelines (VVSG 2.0)', and the Council of Europe's inter-governmental standards for e-voting (CM/Rec (2017)5) to develop the principles, which will guide the design and implementation of an internet voting service in Australia for use by all member electoral commissions.

3.1 ECANZ 11 essential principles for an Australian internet voting service

ENFRANCHISEMENT

1. **Accessibility – as far as is practical, all eligible people should be able to access the internet voting system.**

The internet voting service shall be designed, as far as practicable, to enable eligible voters to vote independently regardless of disabilities, technology or geography. The internet voting service will be an additional and optional service for specific eligible voters to use. It would be offered in conjunction with other pre-existing methods of voting.

2. **Usability – the process of internet voting should be sufficiently easy for eligible people to cast a vote.**

The user interface of the internet voting service should be easy to understand, intuitive, and able to be used by all eligible voters on multiple technology platforms. Information provided may be presented differently depending on the differing technologies and channels which the service can be accessed on. For example, the electoral content presented on an electronic ballot paper will be the same as on the physical paper ballot paper (ensuring impartiality and equitably); however changes may be made in accordance with relevant legislative provisions while ensuring usability on each technology platform.

3. **One person, one vote – the ability to ensure that each eligible elector receives only their voting entitlement.**

The internet voting service should enable each eligible voter to be uniquely identified, ensuring that they are distinguishable from other voters. The service should cater for any legislative requirements around the presentation of identification documents. An eligible voter will only be able to use this channel if they can be uniquely identified this way. The service will check eligibility and only grant access to those that have been authenticated as an eligible voter. The service will have a process to ensure that only one vote per eligible voter is admitted to the count.

INTEGRITY

4. **Security – prevention of loss, corruption or tampering of votes.**

The internet voting service and responsible Electoral Management Body shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify, or otherwise gain knowledge of this data. The authenticity, availability and integrity of the electoral roll and lists of candidates shall be maintained. Only persons authorised by the electoral management body shall have access to the central infrastructure, the servers and the electoral event data.

The audit system should be able to detect voter fraud and provide proof that all counted votes are authentic. The audit system shall be open and comprehensive, and actively report on potential issues and threats. Where incidents that could threaten the integrity of the service occur, those responsible for operating the equipment shall immediately inform the electoral management body. Procedures shall be established to ensure regular installation of updated versions and corrections of all relevant software as the service will need to be continually evolved to meet and protect against potential and actual issues and threats.

The service will encrypt votes if they are to be stored or communicated outside controlled environments. The electoral management body shall handle all cryptographic material securely. Votes shall be kept sealed[2] until after the close of polling.

5. Robustness – the system and processes are not subject to significant interruption or failure.

Robustness applies to people, process and technology. The internet voting service must be available, reliable and secure to ensure that it can function on its own, irrespective of shortcomings in the hardware or software. The technical solution for the service will be peer-reviewed to help ensure availability, reliability, usability and security. The service shall identify votes that are affected by an irregularity so that necessary measures are taken and stakeholders are informed. The electoral management body administering the service will ultimately be responsible for compliance with the above even in the case of failure.

6. Transparency – the system and processes be designed to enable scrutiny, to provide stakeholder confidence.

The internet voting service and accompanying processes will be established with a focus on transparency. The service will ensure that the way in which eligible voters are guided through the internet voting process shall not lead them to vote without due diligence or without confirmation. The service should be designed to allow the voter to express his or her true will. A voter will be allowed sufficient time to consider their choices and will be under no obligation to commit their vote without time for reflection on their choices. Upon casting their vote, the service will verify to the voter that his or her intention is accurately represented and that the vote has been submitted. Any alteration to the voter's vote should be detected by the service.

Voters and third parties should be able to observe the count of the votes and check that only eligible voters' votes are included in the results. The service will provide evidence that only eligible voters' votes have been included and this evidence will be auditable.

Clear and unambiguous information about the internet voting service should be available to the public explaining how to use the service and how the service operates.

The service should be open for verification, assurance and scrutiny purposes. Observers, to the extent permitted by law, shall be enabled to observe, comment on and scrutinise the internet voting component of an election, including the compilation of the results.

7. Independence – accountability for the system and processes shall rest with the Electoral Management Body.

The electoral management body will be accountable for the internet voting service of an electoral event. The electoral management body must be able to put into place assurances that maintain their electoral integrity and independence.

8. Impartiality – the voters' intention should not be affected by the voting service.

An eligible voter's intent should not be affected by the internet voting service. The service will ensure that the way in which voters are guided through the process and the information displayed will not influence their vote.

[2] Sealed is an analogy to the seal on a physical ballot box. This is the term used in the European standards.

The service should be structured to ensure that voters do not miss anything during the voting process. It should provide a means for informal voting by allowing a blank vote to be cast, however advising the voter they would be casting an informal vote and providing them with the option to change their vote if they wish. This provides an equitable approach across channels enabling voters to cast an informal vote via both the service and the paper-based option. Other than a blank ballot paper, all formality rules will be enforced by the service.

9. Accuracy – the service should accurately capture, store and export the voter's intention.

The internet voting service shall provide sound evidence that only votes from eligible voters are included in the final result while de-identifying a completed ballot paper from its voter. The service shall support the voter in marking the ballot paper and accurately store, capture, verify, and export the vote cast. Before an event, the electoral management body administering the service shall satisfy itself that the service is genuine and operates correctly.

The service shall allow and support evaluation regarding the compliance of the service and its related components. This should occur upon introduction, periodically and after significant change to the service has been made.

PRIVACY

10. Privacy of personal information – the system and processes shall maintain the privacy of personal information.

The internet voting service shall process and store, as long as necessary, only the personal data needed for the conduct of the electoral event. The electoral management body administering the service will determine what information is deemed necessary to keep and dispose in accordance with relevant legislative obligations. Any information retained will be secure and any information not required to be retained will be securely disposed of.

11. Secrecy of vote cast – the system and processes shall maintain the secrecy of the votes cast.

The internet voting service shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting process – from pre-polling through to counting of the votes. Votes shall remain sealed until the counting process commences. During completion of the ballot paper, the service will protect the secrecy of the voter's choice. The service should not provide a proof of vote preferences that would facilitate coercion or vote buying.

The service will be able to de-identify a voter from their completed ballot paper to preserve the secrecy of the ballot. The order in which votes are cast shall be mixed so as to deny reconstruction of the order of votes submitted.

It is acknowledged that a tension can arise in giving effect to some of these principles. For example, an appropriate balance needs to be struck between usability and security. Such decisions also need to take into account legislative electoral requirements and the current technological environment.

4. International standards

The internet voting environment is continuing to evolve:

- The Council of Europe (CoE) has recently published new recommendations on standards for electronic voting
- The National Institute of Standards and Technology (NIST) in the USA recently updated the Voluntary Voting System Guidelines (VVSG). These guidelines are currently going through an approval process with the Election Assistance Commission (EAC) which they expect will conclude in 2018.

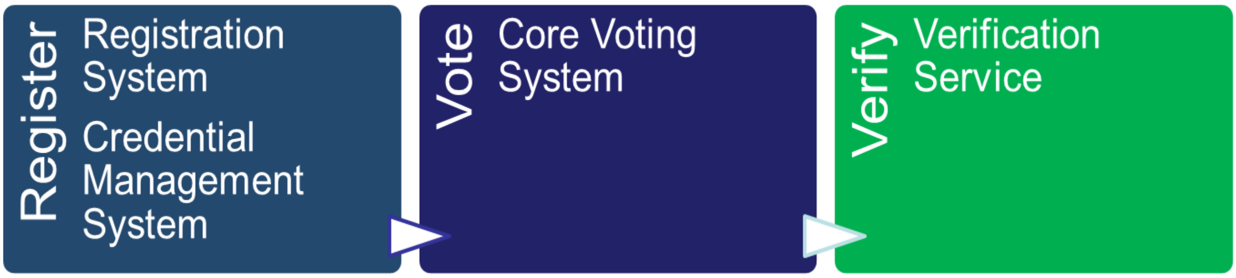
The NSWEC has mapped these international standards and guidelines to the 11 ECANZ principles, as set out in Appendix A. The NSWEC will also analyse the relevance of each standard to the NSW context. This analysis may identify some standards which are inapplicable to the current project. The results of this analysis will be published within the iVote strategy document by mid-2018.

5. Evaluation of research findings

Since the 2015 NSW State General Election, the NSWEC has monitored developments in the field of remote electronic voting. With the commencement of the iVote Refresh Project, we have undertaken an intensive review of academic and real-world projects and proposals, which also included engagement with leading commercial suppliers of remote electronic voting technology. Our own detailed customer research also shows ongoing demand for online voting, in line with general consumer expectation around the availability of online services.

Informed by this work, and the ECANZ principles, NSWEC is now in a position to define requirements for a Request for Proposal (RFP) which we currently plan to release at the end of November or early December 2017.

The current iVote process for voters is split into three steps: Register, Vote and Verify, with the three major system components matching these three steps.



Each of the three components represents different software applications operating in three separate data-centre environments, each provided by different hosting suppliers.

As is the case for the current version of iVote, NSWEC currently intends to retain the separation of Register and Vote components to reduce the risk of a single security breach impacting vote secrecy or vote integrity.

The requirement for separation of Vote and Verify will be re-evaluated once the improved Vote system is determined.

The Vote component will be the primary subject of the RFP mentioned above. The Register and Verify components are currently NSWEC owned software and IP, though NSWEC is open to innovative proposals from potential suppliers of the Vote component in regards to Verify.

Proposals from suppliers may lead to some changes and clarifications to overall design that will then allow the NSWEC to complete the redesign of Registration, ready for redevelopment.

Appendix B lists key common elements of remote electronic voting systems, together with the current NSWEC assessment of options. It reflects the current assessment by NSWEC of various alternatives for verification and other properties of electronic voting systems. It does not specify a particular solution but provides a framework that can be used for examining and developing potential solutions.

Additional context in regards to the adversary model can be found in the *iVote Threat Analysis and Risk Assessment 2015*.

6. Conclusion

The next step for the iVote Refresh Project will be the procurement of software for the voting component, followed by redesign of the registration and verification (unless the selected Voting System proposal includes verification) components. The full strategy document will be published once this work is completed.

The processes of procurement and more detailed design, together with external consultation will further inform the NSWEC's thinking in this area. Consequently, when the full iVote Strategy document is published next year, it may include changes to the positions currently adopted in this document.

Although this brief is not being released as a consultation document, any feedback can be sent to ivote.enquiries@elections.nsw.gov.au.

Appendices

Appendix A: International standards

The NSWEC has mapped both the COE and VVSG international standards and guidelines to the 11 ECANZ principles. The NSWEC will also analyse the relevance of each standard to the NSW context.

This analysis may identify some inapplicable standards and the results will be published within the iVote strategy document by mid-2018.

Enfranchisement

1. **Accessibility.** As far as is practical, all eligible people should be able to access the internet voting system.

   a. CoE | UNIVERSAL SUFFRAGE | Standard No. 2: The e-voting system shall be designed, as far as is practicable, to enable persons with disabilities and special needs to vote independently.

   b. CoE | UNIVERSAL SUFFRAGE | Standard No. 3: Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.

   c. CoE | UNIVERSAL SUFFRAGE | Standard No. 4: Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election in which they are submitting their decision by electronic means is a real election or referendum.

   d. CoE | FREE SUFFRAGE | Standard No. 10: The voter's intention shall not be affected by the voting system, or by any undue influence.

   e. CoE | TRANSPARENCY | Standard No. 31: Member States shall be transparent in all aspects of e-voting.

   f. VVSG | EQUIVALENT AND CONSISTENT | 2: Provide voters with equivalent information and options in all modes of voting.

   g. VVSG | MEETS WEB ACCESSIBILITY STANDARDS | 1: When a voting system uses standard web software platforms (HTML or native apps), the voting system meets all requirements in WCAG 2.0 Level AA [*and*] any applicable requirements in the VVSG.

2. **Usability.** The process of internet voting should be sufficiently easy for eligible people to cast a vote.

   a. CoE | UNIVERSAL SUFFRAGE | Standard No. 1: The voter interface of an e-voting system shall be easy to understand and use by all voters.

   b. CoE | UNIVERSAL SUFFRAGE | Standard No. 2: The e-voting system shall be designed, as far as is practicable, to enable persons with disabilities and special needs to vote independently.

   c. CoE | EQUAL SUFFRAGE | Standard No. 5: All official voting information shall be presented in an equal way, within and across voting channels.

d. CoE | FREE SUFFRAGE | Standard No. 12: The way in which voters are guided through the e-voting process shall not lead them to vote precipitately or without confirmation.

e. CoE | FREE SUFFRAGE | Standard No. 13: The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options.

f. CoE | FREE SUFFRAGE | Standard No. 14: The e-voting system shall advise the voter if he or she casts an invalid e-vote.

g. CoE | FREE SUFFRAGE | Standard No. 16: The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed.

h. VVSG | EQUIVALENT AND CONSISTENT | 1: Provide voters with a consistent experience of the voting process in all modes of voting.

i. VVSG | CAST AS MARKED | 3: The voting system supports the voter in marking the ballot accurately.

j. VVSG | CAST AS MARKED | 4: The voting process helps voters avoid errors that invalidate their ballot, including blank ballots, undervotes, overvotes, and marginal marks.

k. VVSG | MARKED AS INTENDED | 1 PERCEIVABLE: The default system settings for displaying the ballot work for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

l. VVSG | MARKED AS INTENDED | 2 OPERABLE: Voters and poll workers are able to use all controls accurately, and all ballot changes are made with the direct control of the voter.

m. VVSG | MARKED AS INTENDED | 3 UNDERSTANDABLE: Voters can understand all information as it is presented.

n. VVSG | MARKED AS INTENDED | 4 ROBUST: The voting systems hardware and accessories support usability and accessibility requirements while protecting voters from harmful conditions.

o. VVSG | TESTED FOR USABILITY | 1: Completed systems are tested using a wide range of representative voters and poll workers, including those with and without disabilities to measure effectiveness, efficiency, and satisfaction (called “summative usability testing”).

3. **One person, one vote.** The ability to ensure that each eligible elector receives only their voting entitlement.

   a. CoE | EQUAL SUFFRAGE | Standard No. 7: Unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured.

   b. CoE | EQUAL SUFFRAGE | Standard No. 9: The e-voting system shall ensure that only the appropriate number of votes per voter is cast, stored in the electronic ballot box and included in the election result.

   c. CoE | SECRET SUFFRAGE | Standard No. 21: The e-voting system and any authorised party shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify, or otherwise gain knowledge of this data.

Integrity

4. **Security.** Prevention of loss, corruption or tampering of votes.

   a. CoE | EQUAL SUFFRAGE | Standard No. 7: Unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured.

   b. CoE | EQUAL SUFFRAGE | Standard No. 8:The e-voting system shall only grant a user access after authenticating her/him as a person with the right to vote.

   c. CoE | FREE SUFFRAGE | Standard No. 10: The voter's intention shall not be affected by the voting system, or by any undue influence.

   d. CoE | SECRET SUFFRAGE | Standard No. 21: The e-voting system and any authorised party shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify, or otherwise gain knowledge of this data.

   e. CoE | SECRET SUFFRAGE | Standard No. 22: Voters' registers stored in or communicated by the e-voting system shall be accessible only to authorised parties.

   f. CoE | ACCOUNTABILITY | Standard No. 39: The e-voting system shall be auditable. The audit system shall be open and comprehensive, and actively report on potential issues and threats.

   g. CoE | RELIABILITY | Standard No. 40: The electoral management body shall be responsible for the respect for and compliance with all requirements even in the case of failures and attacks. The electoral management body shall be responsible for the availability, reliability, usability and security of the e-voting system.

   h. CoE | RELIABILITY | Standard No. 41: Only persons authorised by the electoral management body shall have access to the central infrastructure, the servers and the election data. Appointments of persons authorised to deal with e-voting shall be clearly regulated.

   i. CoE | RELIABILITY | Standard No. 43: A procedure shall be established for regularly installing updated versions and corrections of all relevant software.

   j. CoE | RELIABILITY | Standard No. 44: If stored or communicated outside controlled environments, the votes shall be encrypted.

   k. CoE | RELIABILITY | Standard No. 45: Votes and voter information shall be kept sealed until the counting process commences.

   l. CoE | RELIABILITY | Standard No. 46: The electoral management body shall handle all cryptographic material securely.

   m. CoE | RELIABILITY | Standard No. 47: Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the electoral management body.

   n. CoE | RELIABILITY | Standard No. 48: The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected.

o. VVSG | HIGH-QUALITY CONSTRUCTION | 4: Perform accurately and reliably in intended environments – ensuring system is free of well-known security vulnerabilities; is able to protect against threats to its software, execution, and/or environment; and ensuring accuracy, data integrity, durability, and safety across all logical and/or physical components and materials.

p. VVSG | ACCESS CONTROL | 1: The voting system identifies users, roles and/or processes to which access is granted and the specific functions and data to which each entity holds authorized access.

q. VVSG | ACCESS CONTROL | 2: The voting system supports authentication mechanisms and allows administrators to configure them.

r. VVSG | ACCESS CONTROL | 3: Default access control policies enforce the principle of least privilege.

s. VVSG | PHYSICAL SECURITY | 1: Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence.

t. VVSG | PHYSICAL SECURITY | 2: Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing.

u. VVSG | DATA PROTECTION | 1: Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

v. VVSG | DATA PROTECTION | 2: The source and integrity of electronic tabulation reports are verifiable.

w. VVSG | DATA PROTECTION | 3: All cryptographic algorithms are public, well-vetted, and standardized.

x. VVSG | DATA PROTECTION | 4: Voting systems protect the integrity, authenticity and confidentiality of sensitive data transmitted over all networks.

y. VVSG | SOFTWARE INTEGRITY | 1: Only software that is digitally signed by the appropriate authorities is installed on the voting system.

z. VVSG | SOFTWARE INTEGRITY | 2: The authenticity and integrity of software updates must be verified by the voting system prior to installation and authorized by an administrator.

aa. VVSG | DETECTION AND MONITORING | 1: Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

bb. VVSG | DETECTION AND MONITORING | 2: The voting system generates, stores, and reports to the user or election official, all error messages as they occur.

cc. VVSG | DETECTION AND MONITORING | 3: Voting systems employ mechanisms to protect against malware.

dd. VVSG | DETECTION AND MONITORING | 4: If the voting system contains networking capabilities, it employs appropriate modern defenses against network-based attacks.

5. **Robustness.** The system and processes are not subject to significant interruption or failure.

a. CoE | EQUAL SUFFRAGE | Standard No. 6: Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the result.

b. CoE | FREE SUFFRAGE | Standard No. 11: It shall be ensured that the e-voting system presents an authentic ballot and authentic information to the voter.

c. CoE | RELIABILITY | Standard No. 42: Before any e-election takes place, the electoral management body shall satisfy itself that the e-voting system is genuine and operates correctly.

d. CoE | RELIABILITY | Standard No. 49: The e-voting system shall identify votes that are affected by an irregularity.

e. VVSG | HIGH-QUALITY CONSTRUCTION | 1: Use trustworthy materials, methods, standards, and best practices – including accepted and appropriate tools/standards for constructing hardware and software, protocols for constructing and performing telecommunications, as well as best practices for quality assurance and configuration management.

f. VVSG | HIGH-QUALITY CONSTRUCTION | 2: Organize the elements and logic of the system meaningfully – ensuring logic that is clear, meaningful, and well-structured; system organization that is simple, modular, and robust to change; and hardware, telecom, data, and related infrastructure that can support system processes and functions with integrity.

g. VVSG | HIGH-QUALITY CONSTRUCTION | 3: Handle errors actively and appropriately, recovering from failure gracefully –processing or avoiding well-known errors and/or software bugs; and avoiding single points of failure that could cause complete loss of voting capabilities.

h. VVSG | SCALABLE | 1: The system provides sufficient technical and physical capacity to accommodate large and complex ballot styles, growing language needs, and large numbers of voters and precincts and consolidation of elections with local districts and municipalities.

i. VVSG | SCALABLE | 2: The system provides the ability to adapt to different election types, environments, and changing regulatory requirements.

j. VVSG | AUDITABILITY | 3: Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

6. **Transparency.** The system and processes be designed to enable scrutiny, to provide stakeholder confidence.

a. CoE | FREE SUFFRAGE | Standard No. 15: The voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable.

b. CoE | FREE SUFFRAGE | Standard No. 17: The e-voting system shall provide sound evidence that each authentic vote is accurately included in the respective election results. The evidence should be verifiable by means that are independent from the e-voting system.

c. CoE | FREE SUFFRAGE | Standard No. 18: The system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system.

d. CoE | REGULATORY | Standard No. 27: Member States that introduce e-voting shall do so in a gradual and progressive manner.

e. CoE | REGULATORY | Standard No. 28: Before introducing e-voting, member States shall introduce the required changes to the relevant legislation.

f. CoE | REGULATORY | Standard No. 30: Any observer shall be able to observe the count of the votes. The electoral management body shall be responsible for the counting process.

g. CoE | TRANSPARENCY | Standard No. 31: Member States shall be transparent in all aspects of e-voting.

h. CoE | TRANSPARENCY | Standard No. 32: The public, in particular voters, shall be informed, well in advance of the start of voting, in clear and simple language, about: any steps a voter may have to take in order to participate and vote; the correct use and functioning of an e-voting system; the e-voting timetable, including all stages.

i. CoE | TRANSPARENCY | Standard No. 33: The components of the e-voting system shall be disclosed for verification and certification purposes.

j. CoE | TRANSPARENCY | Standard No. 34: Any observer, to the extent permitted by law, shall be enabled to observe and comment on the e-elections, including the compilation of the results.

k. CoE | TRANSPARENCY | Standard No. 35: Open standards shall be used to enable various technical components or services, possibly derived from a variety of sources, to interoperate.

l. CoE | ACCOUNTABILITY | Standard No. 39: The e-voting system shall be auditable. The audit system shall be open and comprehensive, and actively report on potential issues and threats.

m. CoE | RELIABILITY | Standard No. 43: A procedure shall be established for regularly installing updated versions and corrections of all relevant software.

n. VVSG | HIGH-QUALITY CONSTRUCTION | 5: Support auxiliary functions necessary for operations and transparency such as for supporting auditing and testing – ensuring these aims are achievable via supporting structures, functions, and data; are implemented in software, hardware, telecom, and/or other infrastructure; and are able to support accurate identification, tracking, and management of hardware, software, and data across the system lifecycle.

o. VVSG | EASE OF EVALUATION | 1: Ensure reviewers can clearly identify all essential elements of a specified system in evaluated systems – including identification of unique election/auxiliary processes and functions; wherever they are implemented in software, hardware, telecom, data, and/or other technology layers of the system; and with an ability to record and track these identifications.

p. VVSG | EASE OF EVALUATION | 2: Ensure reviewers can clearly distinguish correct from incorrect system configurations in evaluated systems wherever they are implemented in software, hardware, telecom, data, and/or other technology layers of the system; and with an ability to record and track these distinctions.

q. VVSG | TRANSPARENT | 1: The processes and transactions associated with the voting system are easy for the public to understand and verify.

r. VVSG | TRANSPARENT | 2: Voting system data is easily accessed via imports/exports and reports.

s. VVSG | TRANSPARENT | 3: Data reported by the voting system is in a publicly documented format.

t. VVSG | TRANSPARENT | 4: Data used in critical device operations such as for cast vote records, tabulations, and event logs includes all elements necessary for verification of the data, and analysis and auditability of the operations.

u. VVSG | INTEROPERABLE COMPONENTS | 1: Voting system data is in an interoperable format that is common across manufacturers and documented for each device by the manufacturer.

v. VVSG | INTEROPERABLE COMPONENTS | 2: Formats for other types of data use industry standard formats where applicable, but in any case, use formats that are publicly available.

w. VVSG | INTEROPERABLE COMPONENTS | 3: Components of voting systems interoperate without the need to replace the entire system or undertake costly system modifications or impact security.

x. VVSG | INTEROPERABLE COMPONENTS | 4: Widely used hardware interfaces and communications protocols are used where possible.

y. VVSG | AUDITABILITY | 1: An undetected error or fault in the voting system's software or hardware is not capable of causing an undetectable change in election results.

z. VVSG | AUDITABILITY | 2: The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities.

aa. VVSG | AUDITABILITY | 4: The voting system supports efficient audits.

7. **Independence.** Full control of the system and processes shall rest with the Electoral Management Body.

   a. CoE | REGULATORY | Standard No. 29: The relevant legislation shall regulate the responsibilities for the functioning of e-voting systems and ensure that the electoral management body has control over them.

   b. CoE | ACCOUNTABILITY | Standard No. 36: Member States shall develop technical, evaluation and certification requirements and shall ascertain that they fully reflect the relevant legal and democratic principles. Member States shall keep the requirements up to date.

8. **Impartiality**. The voters' intention should not be affected by the voting system.

   a. CoE | FREE SUFFRAGE | Standard No. 10: The voter's intention shall not be affected by the voting system, or by any undue influence.

b. CoE | SECRET SUFFRAGE | Standard No. 24 The e-voting system shall not allow the disclosure to anyone of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.

9. **Accuracy.** The system should accurately capture, store and export the voters' intention.

   a. CoE | ACCOUNTABILITY | Standard No. 37: Before an e-voting system is introduced and at appropriate intervals thereafter, and in particular after any significant changes are made to the system, an independent and competent body shall evaluate the compliance of the e-voting system and of any information and communication technology (ICT) component with the technical requirements. This may take the form of formal certification or other appropriate control"

   b. CoE | ACCOUNTABILITY | Standard No. 38: The certificate, or any other appropriate document issued, shall clearly identify the subject of evaluation and shall include safeguards to prevent its being secretly or inadvertently modified.

   c. VVSG | CORRECT IMPLEMENTATION | 1: Carry out election operations completely and accurately across the entire election process – supporting the integrity and maintainability of the entire process and data across hardware, software, telecom, data, and/or other technology layers of the system.

   d. VVSG | CORRECT IMPLEMENTATION | 2: Carry out election processes completely and accurately under realistic operating conditions – including correct operation under expected workloads, expected environmental conditions, and means of data transfer.

   e. VVSG | CORRECT IMPLEMENTATION | 3: Carry out election processes completely and accurately carry across the entire system lifecycle –ensuring election processes remain correct in definition and execution no matter [whether] how the system lifecycle processes may change (i.e., specification, implementation, testing, operations, or maintenance processes) and regardless of whether this is occurring in hardware, software, telecom, data, and/or other technology layers of the system.

Privacy

10. **Privacy of personal information.** The system and processes shall maintain the privacy of personal information.

   a. CoE | EQUAL SUFFRAGE | Standard No. 6: Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the result.

   b. CoE | SECRET SUFFRAGE | Standard No. 19: E-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure.

   c. CoE | SECRET SUFFRAGE | Standard No. 23: An e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties.

   d. CoE | SECRET SUFFRAGE | Standard No. 25: E-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected.

e. CoE | SECRET SUFFRAGE | Standard No. 26: The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous.

f. VVSG | CAST AS MARKED | 1: The voting process preserves the secrecy of the ballot.

g. VVSG | BALLOT SECRECY | 1: Ballot secrecy is maintained throughout the voting process.

h. VVSG | BALLOT SECRECY | 2: Records, notifications and other election artefacts produced by the voting system do not reveal the intent, choices, or selections of any identifiable voter.

11. **Secrecy of vote cast.** The system and processes shall maintain the secrecy of the votes cast.

a. CoE | SECRET SUFFRAGE | Standard No. 20: The e-voting system shall process and store, as long as necessary, only the personal data needed for the conduct of the e-election.

b. VVSG | CAST AS MARKED | 2: The voting system ensures that ballot selections, interface options, voter identity and information about voters are kept private.

Appendix B: Verification and other options

B1: Verification options

While not available for voting using paper ballots, verification is considered an important property for electronic voting and various protocols for electronic voting take different approaches to the fundamental goal of assuring integrity.

Verification is typically considered in three parts:

1. Cast as intended (the vote preferences are what the voter wants to vote)
2. Recorded as cast (the system has actually saved the vote preferences correctly)
3. Counted as recorded (the saved vote preferences are all counted correctly)

The first two are performed by the voter; the third should be open to anyone to confirm.

Voting protocols and verification options are the subject of much academic discussion and real-world implementations have typically needed to strike an appropriate balance between three requirements: proof against vote tampering, secrecy of the vote and usability/accessibility for the voter.

Solution options	Pros	Cons	Conclusion
1. INDIVIDUAL VERIFICATION (Cast as intended and Recorded as cast.)	Provides the means for the voter to be able to verify the vote. Improves transparency and voter confidence in the system. Protects against Malware on voting device or man-in-the-middle attacks.	Additional steps for the voter in the voting processes. Potentially allows coercer or vote buyer to verify that vote was cast as instructed. Implementations could unintentionally 'leak' voter preference information.	Verification is important for election assurance. Must not compromise ease of use for the voter and should be usable by voters with disabilities. A 2013 study concluded that coercion and vote-buying are not significant risks in the Australian context, which should be taken into account when evaluating verification approaches.
1.1 Protection for votes being cast from an insecure platform.			Cannot prevent malware on a voter’s device.
• Use a different device for voting and verification.	Both devices have to be infected, which is less likely than one device being infected. Different device could be a different channel, e.g. phone vs web.	More complex for voter. Might be difficult to be sure voter does use a different device. If abroad, access to a different device may be a barrier.	Preferred approach but needs to address usability in the way implemented.
• Use hardware token device.	Isolated therefore relatively more resilient to compromise	Not viable just for elections due to cost, logistics, etc.	Not considered in the NSW context since the cons significantly outweigh the pros.
• Use return codes (see 1.3).			

Solution options	Pros	Cons	Conclusion
1.2 Decryption of vote. *(The vote is decrypted for the voter to verify versus providing the encrypted vote or a hash of the encrypted vote.)*	Simpler for the voter as the vote cast is not obscured.	Could be used as proof of vote to a coercer or vote buyer, however proving your vote in other voting channels is not easily prevented (e.g. taking a photo in the polling place) so not necessarily weakening the current state when compared against other voting channels.	Prefer decrypting the vote for verification because ease of use is important and coercion risk is low.
1.2.1 Location of decryption.			
• Server	All processing is done on the server and the requirements on the client side are minimum.	Decryption of the vote on the server could provide the means for an insider to learn how a particular voter has voted.	Server-side decryption is not ideal. If IVR verification is necessary for voters with disability, then this is an implementation option.
• Device	Could increase the security by ensuring that the vote is decrypted on the voter's device and the server does not learn the key to decrypt.	Requires the voter's device, which may not be secure, to be able to perform the decryption process.	Decryption on voter's device is preferable to server-side decryption, assuming that usability is not significantly compromised.
1.2.2 Key for decryption.			
• Receipt numbers	Ease of use. Provides the means for the voter to be able to verify the vote. Dependent on the design of the voting protocol it could also be used to mislead a coercer with a false proof.	If malware corrupts a voting session then it could also corrupt the receipt number. Receipt number could be obtained by a coercer or provided to a vote buyer as proof of vote.	The current iVote system uses the receipt number for vote decryption but other approaches are likely to offer improvements. (It also uses the receipt number for counted/tallied as recorded.)

Solution options	Pros	Cons	Conclusion
• Token generated when vote encrypted (a receipt or otherwise) that can be used for verification - either for immediate use or can be saved	Generated and used on device at time of vote encryption. Used immediately afterwards for verification. Not saved on device afterwards.	If malware corrupts a voting session then it could also corrupt delivery of the token, unless delivered to alternate device. Token could be obtained by a coercer or provided to a vote buyer as proof of vote.	Variations on the current receipt number approach may offer significant improvements and NSWEC does not have a preferred approach, but is open to innovative proposals.
• Private key	A digital certificate on voter's device (like digital driver licence) would be used to decrypt the vote and could be seamless for the voter.	Delivery (prior to voting session) and security of the certificate would need to be resolved.	Could offer the best solution but NSWEC does not have a preferred approach and is open to innovative proposals.
1.3 Use of return codes.	Allows verification on same device as used to vote by using a set of secret, unique 'return codes' for each voter. Randomised codes for each elector allow vote preferences to be obscured during voting and verification to maintain secrecy of the vote. Return codes allow mandatory verification as the system can enforce checking the codes as part of vote submission steps. Has been used successfully in Norwegian and Swiss elections.	Preparation and distribution of personalised return codes may be high cost with significant risk of errors occurring. More complex for voters to understand and potentially use. Provision of the voter's unique codes to a coercer or vote buyer destroys any benefits to vote secrecy. The three-day time frame (from candidates being finalised to start of voting) to deliver codes (via alternative, safe channel) may make this impossible.	A suitable approach, though concerns over usability and voter understanding need to be addressed as well as secure delivery of return codes within available time frame. This could be an option for NSW if all concerns are addressed.

Solution options	Pros	Cons	Conclusion
1.4 Distribution method. *(For return codes, or for private key for decryption or token.)*			As for delivery of voting credentials, NSWEC expects that a number of options will need to be supported. Private keys are to be handled carefully.
- Email	Email is widely acceptable, cost effective and good ease of use.	Considered not to be secure channel for communication although a signature could be added with the public certificate posted on the iVote landing page.	A possible method, though not the best. Support of this as an option might be necessary to maximize timeliness and accessibility.
- SMS	SMS is widely used and acceptable. Cost effective if implemented through a SMS service platform. Proof of identity required to obtain Australian mobile number.	Considered not to be secure channel for communication. Outside of Australia, proof of identity for SIM activation is not mandatory.	Preferred method for return codes due to immediacy of communication and independence from voting channel.
- Post	Mature and accepted channel.	Expensive and not always reliable service with mailboxes being insecure for many people. Not very useful for delivery of private key.	Time frame of three days from candidates being finalised to start of voting limits viability of post for return codes. Accessibility an issue.
- Voting device	No need for additional step. Uses existing connection with voter's device. Key is only known to the voter.	More difficult to support phone voting. Vulnerable to an insecure environment on voter's device.	As currently used to deliver receipt code. Preferred method to maintain voter secrecy for private key/token.

Solution options	Pros	Cons	Conclusion
- Secure app	More opportunity to take advantage of mobile platform security features. Receipt history could be controlled. Could be used to warn the voter if a vote was cast in their name by an attacker. Direct channel to communicate to the voter.	Cost and time for development of app. Requires the voter to install an app that may only be used once every 4 years, however a multi-function elections app supporting various features of local govt., state and federal elections may address this. Cost and time for integration with the verification system. Could be a single point of security failure.	Option not ruled out by NSWEC but seems unlikely to be a good fit to requirements for 2019.
- Phone	Ease of use for Voters. Human interaction can deliver confidence in the system.	Cost of calls is higher than other channels. Scalability issues compared to other channels.	Just as for credentials, this may need to be an option for certain voters with disabilities.
1.5 Other verification methods.			NSWEC is open to innovative proposals provided overall objectives and priorities are also met.
- Trial vote credentials for verification. (The voting system cannot distinguish between actual and test votes.)	Allows voter to confirm system via a 'test vote' then make their actual vote. Could be integrated with use of test votes prior to start of voting. Test votes can be published on bulletin board.	Potential confusion between test vote and real vote. Will many voters bother to cast a test vote?	Extra effort and potential confusion, plus the likelihood that few voters will bother with a test vote mean this is not viewed as a suitable approach for voters. However, it could be an approach for operational testing (logic and accuracy) prior to go live.

Solution options	Pros	Cons	Conclusion
• Cut-and-choose. An approach (generic 'Benaloh challenge') whereby a vote can be tested (similar to with trial credentials) by the voter	Here a voter can choose to test a vote after casting it. This verifies the vote was as cast, but then destroys the vote and the voter casts a new vote, which can also be tested or left as the submitted vote.	Potential confusion to voters who might challenge and then not recast the vote. Uncertain that many voters will bother to challenge a vote. Limited protection for voter's insecure platform.	Extra effort and potential confusion, plus the likelihood that few voters will bother to challenge a vote mean this is not viewed as a suitable approach.
• Encrypt vote a second time on a different device (Estonia 2013) with vote encryption parameters sent via camera	No need to decrypt the vote for verification.	Accessibility issues. Potential performance implications for NSW Legislative Council elections with 300+ candidates below-the-line.	As it stands, not suitable for a key cohort of iVote.
• Alternative verification methods			None identified that are suitable for remote voting, but NSWEC may receive proposals with innovative ideas.
1.6 Recoverability if verification fails.	Avoids doubts in cases of failed verification by identifying the source of failure, including a falsified verification result.	Additional complexities and steps could impact usability for voters.	Current system only supports revoting and NSWEC expects improvements to this for 2019.

Solution options	Pros	Cons	Conclusion
1.7 Mandatory or Optional verification.	Mandatory ensures a higher degree of assurance for the election. Optional allows the voter a simpler process, like paper voting, if they are not interested in verifying their vote.	Mandatory forces voters to perform additional steps that are not part of paper voting. Additional mechanisms required to be able to address claims of verification failure. Optional may not achieve enough verifications to gain desired statistical confidence level. The profile of those that choose to verify is likely to represent those who are less likely to be affected by malware.	Ideally, the objectives of assurance can be obtained without compromising usability for voters.

2. UNIVERSAL VERIFICATION (Counted as Recorded)	Assurance that there was no tampering with the votes cast. Reassures voters that votes were counted as cast.	Requires additional processes. Complexity and cost of implementation.	Verification is important for election assurance.
2.1 Mixing.	After mixing, no vote can be linked to the voter. Increases trust in the vote secrecy of the system.	Requires additional processing power. Mixing process could corrupt or exclude valid votes.	Stripping voter identifying information from votes without then mixing them is inadequate.
• Verifiable With Mathematical proofs	Mathematically provable mix-nets exist that allow proof of the mixing with all votes being correctly emitted from the process.	Need to ensure that the mixing performance is sufficient for the post-election timeline Proof relies on specialised mathematical and cryptographic knowledge to confirm.	Assurance of the mixing process is worthwhile, assuming it introduces no other significant risks or delays to the election results.

Solution options	Pros	Cons	Conclusion
2.2 Decryption proofs.	Mathematical proofs of correct decryption of votes can be achieved with certain cryptographic schemes.	Computationally heavy for the large number of votes that NSW will process. Proof relies on specialised mathematical and cryptographic knowledge to confirm.	Assurance of the decryption process is worthwhile, assuming it introduces no other significant risks or delays to the election results or weakens vote secrecy protections.
2.3 Use of Bulletin Board (BB).	Increases transparency and trust in the system through scrutiny. Supports end-to-end verifiability.	Increases the complexity and cost of implementation. May expose election data to external attack. Requires additional security implementations.	Publishing the vote in the clear would allow a running count and is not permissible under NSW law. Publishing other vote data is permissible and could enhance transparency and scrutiny of the system.
• Publish hash of encrypted vote	The fingerprint of the vote can prove no subsequent tampering. Content of the vote cannot be determined from the hash.	Decryption of the vote for verification is separate from BB.	A hash or similar derivative of the vote being saved on a public bulletin board could be a useful assurance measure for the system.
• Publish the encrypted vote	Voter can verify the vote on the BB matches the vote cast. The encrypted vote can prove no subsequent tampering.	For the voter to verify the encrypted vote on the BB it must be stored with a connection to the voter. Votes encrypted with current algorithms could be vulnerable to attack in the future and once all encrypted votes are published, not all copies can be destroyed after the election.	The encrypted votes being saved on a public bulletin board could be a useful assurance measure for the system, but would need to be achieved in a way that doesn't compromise secrecy of the votes, either during the election or in subsequent years.

Solution options	Pros	Cons	Conclusion
2.4 Vote comparison.	For the current iVote system, a comparison of votes to be counted with the votes in the verification system provides assurance that votes being counted match votes as cast. Means an attacker must synchronously corrupt both pools of votes, whilst avoiding detection of changes through voter verifications.	Level of assurance depends on percentage of votes verified by voters. Needs to be done in a way that prevents linking the decrypted vote with the voter.	The current approach of comparing two separate pools of votes at the close of the election is a valuable assurance mechanism and a version of this may be a feature in future versions of iVote.
2.5 Post votes in the clear after the election with privacy preserving tracker id (e.g. Selene protocol).	Allows verification after voting closes, which may improve assurance of the results.	Verifying after the election closes means that nothing can be done by a voter who discovers their vote was corrupted by malware, however publishing the vote in the clear before voting closes would allow a running count and is not permissible under NSW law.	This might add value as part of a protocol that also allows voter verification before the close of voting, though it is unlikely that voters would adopt such a complex process.

B2: Other options

This table reflects the current assessment by NSWEC of various possible approaches for voting systems aside from verification, such as encryption methods, open source code and credential strength.

Solution options	Pros	Cons	Conclusion
1. VOTE ENCRYPTION	Ensures the cast vote is secure. Supports vote secrecy. Increases the voter's trust.	Server or client device need capability to perform the encryption, with appropriate processing power.	Vote encryption is a necessity whenever some connection to the voter is retained, as occurs in the current iVote system to allow later removal if the voter has had a postal or pre-poll vote accepted.
1.1 Encryption approach.			Well known encryption approaches are preferred by NSWEC, including signing of encrypted votes.
• Use of public, standardised, well-vetted algorithms	Improves transparency and scrutiny of the system. Performance of cryptography will be more reliable.	Weaknesses of the encryption algorithms are as well-known as the strengths, leaving open the possibility that adversaries have created or acquired "zero day" attacks on standard algorithms that they may unleash on election day.	Use standard algorithms.
• Modular design that supports incorporating more advanced algorithms	Simpler to adapt to advances in cryptography.	No cons perceived by NSWEC.	Adopt a modular design.
• Includes signing	Signing with a certificate issued to the voter may improve integrity.	Signing creates a tenuous link to the voter, but any risk is outweighed by the assurance of validity of the encrypted votes in the digital ballot box.	Consideration will be given to including signature technology to protect voting integrity.

Solution options	Pros	Cons	Conclusion
- Use of unique, proprietary encryption algorithms	No pros perceived by NSWEC	Security is not improved through obscurity and external experts would be unable to review the cryptography of the system. Incorporation of proprietary algorithms increases the risk of challenges with compatibility	Use standard algorithms.
- Present and encrypt the ballot before logon as per Helios	The ballot presentation and encryption is open to public scrutiny. Reduces risk of malicious server manipulating ballots. More adaptable to alternative verification mechanisms.	The voter has to correctly select their district for voting, easier for state by-election, harder for local government. However, smart selection of district based on entering address could alleviate this.	Usability would be a critical criteria to meet.
1.2 Location (of encryption).			Probable that both client-side and server-side vote encryption need to be supported.
- Encrypt on device	Improves security as all sensitive data is sealed and protected prior to transfer from the device.	Requires moderate processing to take place on the device. Voter's device must be compatible with the encryption algorithm.	Encrypt on the device.
- Encrypt on server	Server-side encryption is the only option for IVR phone voting. Server-side encryption could prevent some web voters from being disenfranchised when they don't have access to a device capable of the encryption.	The data is protected during transfer however is received in the clear on the server, which makes the solution more susceptible to insider attacks, which is not ideal and should be accompanied with other mechanisms that guarantee integrity and validity of the vote	Server-side encryption is acceptable for IVR voting. Use of device-side encryption so far, indicates the option to allow a web voter to proceed with server-side encryption should not be offered.

Solution options	Pros	Cons	Conclusion
- Not encrypt	Some protocols post unencrypted votes that have no link to the voters - this can give assurances against tampering.	This conflicts with the NSW requirement that no counting is allowed prior to the close of voting.	This would not be acceptable to NSW as it would allow counting prior to the close of voting.
3. RE-VOTING *Can be offered as multiple votes per credential with last vote counting, or as ability to get new credential to vote and cancel old vote (as per current system).*	Ensures the Voter can correct their selection by re-voting if verification shows it has been corrupted. In case of coercion the voter can recast their vote. Vote buyer cannot be certain voter will not revote afterwards.	Additional complexity to ensure only one vote per person. Possible misperceptions of this feature by individual voters or the public. Performing re-voting in a verifiable way. Revote processes may be confusing to some voters.	This feature is a requirement due to offering verification, because a voter finding their vote is not as cast must be allowed to fix the situation.
4. DISPUTE RESOLUTION *Enables a failure in the voting protocol to be detected and the offending party to be identified and made accountable. Each failure should have a resolution process.*	Avoids doubts in cases of failures by identifying the source of failure, including any falsification.	Complex to achieve in practice and tied to some extent to the approaches selected.	NSWEC is seeking to improve accountability in the event of voting protocol failure.
5. ROADMAP FOR ADDRESSING LIMITATIONS	Reduce refactoring work to subsequently adopt requirements that are not delivered for 2019.	Could put iVote Refresh delivery for 2019 election at risk if too much effort spent on future-proofing.	As it is unlikely the 2019 solution will include all requirements, NSWEC will document and publish a roadmap.

Solution options	Pros	Cons	Conclusion
6. SCALABILITY	The voting protocol and cryptography selected for iVote should accommodate the 500,000 votes that are estimated to be collected electronically in 2019, with ample 'headroom'.	Some voting protocols do not appear to scale well.	NSWEC will need all components of the system to scale efficiently and cost-effectively beyond the 500k voters estimated for 2019.This may limit the voting protocols that will be suitable noting that techniques that parallelise expensive computations should be used.
7. MODULAR	Ease of adaptability increases as the design becomes more modular. Reduce risk of vendor lock in.	Existing code may not follow a modular design which could introduce regression and deliver risk if it was refactored.	Modular design and development to be followed and existing product should be opportunely migrated to a more modular design according to the product road map.
8. OPEN INTERFACE SUPPORT			The format of messages transferred on voting interfaces is unambiguously documented.
• For voting (encrypted votes)	Allows independent vote collection servers to participate in an election.	Defining an open interface will incur extra cost/effort and might be less flexible in adapting to future needs.	The encrypted vote should be produced and the format unambiguously documented. For the number of electors projected for 2019 we do not anticipate deploying independent voting servers. However this will be included in the roadmap.
• For distribution to Assurance/WBB	Allows independent processing of the encrypted votes, eg as a node in the mix-net.	Defining an open interface will incur extra cost/effort and might be less flexible in adapting to future needs.	The encrypted vote should be produced and the format unambiguously documented.

Solution options	Pros	Cons	Conclusion
- For decrypted votes	Allows independent numerical analysis of the votes.	Defining an open interface will incur extra cost/effort and might be less flexible in adapting to future needs.	The decrypted vote must be produced and the format unambiguously documented.
9. ACCESSIBLE VOTING PROTOCOL	Targets a key cohort of the users of iVote.	Making voting systems accessible can cause conflicts with making them sufficiently secure.	Where conflicts arise, the solution should give the voter an informed choice in terms of balancing security versus accessibility, eg length of credentials.
10. VOTING CHANNELS			iVote offers web and telephone (automated & operator) voting.
- Web	Accounts for over 95 per cent of votes on iVote and is readily accessible.	The large variety of devices and software in use raises issues of support and risk of vulnerabilities or malware.	Essential and primary channel for iVote.
- Interactive Voice Response (IVR). Automated telephone voting using DTMF [touch-tone] control	Accessible to people who have difficulty accessing websites, especially people who are blind, with low vision or illiterate (one of the four eligibility groups for iVote).	Small part of iVote usage, yet adds significant complexity and costs.	Despite widespread web usage and acceptance of operator assisted telephone voting, NSWEC expect to continue offering IVR phone voting.
- Polling Place/Attendance voting	Verification is achievable through VVPAT (Voter Verifiable Paper Audit Trail).	Not a viable mechanism for the voting cohorts targeted by the legislation.	NSWEC would be interested in voting system options for attendance voting.
11. EASILY EXPLAINABLE VOTING PROTOCOL	A voting protocol, including verification, which is easily understood by stakeholders such as voters, candidates and the media, is to be preferred over protocols that are harder to understand.	All electronic voting requires expertise to understand the detail and it is probable that some careful explanation will be required of any voting protocol.	NSWEC has a preference that the process and security of electronic voting can be reasonably understood by the average voter.

Solution options	Pros	Cons	Conclusion
12. AUTHENTICATION			
• Credential strength ok for web	Credentials for web voting can utilise all keyboard characters to be stronger and better resist attacks. (for the current iVote system, just numbers are used).	The benefit of a voter's credentials being usable for both phone and web voting may be lost as web credential strength is increased.	NSWEC selected the current credentials, of a combined six digits and eight digits, in 2010. Current security recommendations indicate that credential strength should be increased to at least 128 bits.
• Credential strength ok for IVR	IVR phone voting requires numeric credentials, which need to be longer to obtain the same degree of security.	The number of digits in credentials may be limited for usability, meaning lower strength credentials.	NSWEC recognises that it may be necessary to have separate, less strong credentials for IVR voting to maintain usability. (noting that the increased risk of brute force attack is offset by the lower susceptibility of the voting method)
• Multi-factor	An additional factor, such as the voter's mobile number could be utilised when logging in to vote. SMS is now commonly used this way by banks and others.	A mobile phone number is a direct link to the voter's identity and a bigger risk to vote secrecy than random credentials. Phone numbers are routinely spoofed by sophisticated attackers.	This might be a useful option for registration of electors to use iVote. Any use for the voting step would need very careful consideration with one option being to send the authentication code via the separate iVote component that delivers credentials.

Solution options	Pros	Cons	Conclusion
- Federated, eg OpenID	A voter who is already signed in to a service, such as a government identification account, could skip some identification steps.	Availability, features and usage of such IDs is changing rapidly as they develop. The value of the external ID needs to be clearly understood. The authentication method could reveal the voter's identity and therefore violate vote secrecy.	NSWEC is interested in opportunities to leverage the identification of voters through federated services.
- Delivery methods	If various methods are offered then the elector is likely to have a suitable method available, though SMS might be the most preferred method.	Some delivery methods are less reliable, such as post, but may still need to be offered to suit elector circumstances.	NSWEC is comfortable with the current mix of delivery methods for credentials, which includes SMS, email, post and outbound calls made by human operators.
13. FAULT TOLERANT VOTING PROTOCOL (In the sense that the result is unaffected if one of the voting servers is corrupted.)	Improves integrity of the voting system.	Requires significant additional resources to implement.	Desirable for 2019 and should be allowed for in the design.
14. MULTI-VOTING PROTECTION			
- Prevention of multi-voting within electronic voting system	The challenges are well-understood within an electronic voting system.	Requires strong credential systems. Does not address multi-voting with other methods of voting.	NSWEC currently achieves this with iVote.

Solution options	Pros	Cons	Conclusion
• Prevention of multi-voting across different methods of voting. (By connecting voter mark-offs across all methods in real time or limiting all opportunities for multi-voting by restricting voter options)	Facilitates enforcement of the “one elector, one vote” principle.	Limiting voting methods reduces electors’ flexibility. Connecting voter logs electronically introduces another threat surface. Auditing adds time and complexity to the voting process.	NSWEC currently achieves this across postal, iVote and pre-poll voting, but the use of paper rolls for mark-off in voting centres on election day means there is limited multi-vote protection for election day voting. NSWEC monitors multi-voting and considers that current prevention measures address this issue.
15. SOFTWARE INDEPENDENT APPROACH FOR DEMONSTRATING ELECTION INTEGRITY	Provides assurance of election integrity through end to end verifiability.	For remote electronic voting depends on cryptographic mechanisms which difficult to explain to the general public.	NSWEC expects the iVote solution to be software independent.
16. OPEN SOURCE SOFTWARE **IN PRACTICE, SOURCE CODE PUBLICATION WOULD ALSO SATISFY THIS OPTION**	Transparency. The software should be more secure and robust with many independent people reviewing the source code.	Commercial software will come with limitations on disclosure. Minimal real improvements in security achieved in practice for voting systems. Potential enablement of attackers. Costs of publishing source code and responding to queries raised. There is limited demand from the general public to justify the costs of making commercial software open source.	In the absence of well accepted open source internet voting projects, NSWEC will need to consider commercial software amongst the options for iVote for which the vendors may not be ready to make fully open source. NSWEC will continue to pay for expert reviews of source code and will also consider the cost-benefit of publication, in the context of negotiations with the vendor.

Solution options	Pros	Cons	Conclusion
17. PUBLICATION OF CONTRACTS	Transparency.	Vendors may be reluctant to disclose contract details and Govt. procurement rules routinely include protections of commercial information. The tender documents are already public.	Current NSW Procurement policy is that only the vendor name, total contract price and a brief description of the services is made public. NSWEC will explore whether anything additional can be published.
18. SUPPORT FOR MULTIPLE SIMULTANEOUS ELECTIONS	NSWEC often runs more than one election within the same time frame and if iVote was, for example, extended to local government elections, it may need to run multiple election events and election types at the same time.	Supporting more than one election at a time will add to system complexity.	The system should have the ability to support both local government elections and State elections. (It should be noted that any decision about the future use of iVote at local government elections is a matter for the NSW Government.)
19. COMPLIANCE AND ALIGNMENT WITH INTERNATIONAL STANDARDS AND FORMATS (EML, COE, VVSG, WCAG, ETC)	Alignment with standards will result in a better quality solution.	In some cases the benefits are marginal. In some cases it will not be practical to implement for SGE 2019.	NSWEC will be looking for solutions that maximise compliance and alignment with standards based on benefit and timescale to implement.
20. CERTIFICATION AGAINST SET OF INTERNATIONAL STANDARDS BY INDEPENDENT BODY	Increased public confidence in fitness for purpose.	A custom Common Criteria Protection Profile would need to be established Identifying suitably qualified onshore independent body to perform the testing cost-effectively.	At this time, it is unlikely that NSWEC will pursue independent testing for 2019. Any internal testing will follow established Common Criteria Protection Profiles such as for operating systems.

Solution options	Pros	Cons	Conclusion
21. VOTING CLIENT IN BROWSER VERSUS AN APP	Support for multiple device types/environments is much simpler.	Easier to support secure features of voting clients, for example Trusted Execution Environment For a one off vote, from the voters point of view, could be put off by having to download an app.	Expected that the vast majority mobile users to use web browser to vote however would be interested in mobile options.
22. HIGH ASSURANCE DEVELOPMENT	Demonstrable robustness of voting protocol, overall system.	Effort level required to achieve.	NSWEC is interested in seeing options for applying this to critical areas.