NSW Electoral Commission

iVote® Project

iVote® System Security Implementation Statement

2 March 2014

New South Wales Electoral Commission
ABN. 94 828 824 124

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

Document Information

Criteria	Details
Document	iVote® System Security Implementation Statement
Document author	NSWEC
Document owner	Ian Brightwell
Document location	

Contents

1 Commissioner’s Foreword

The advance of online voting improves access to voting for groups of electors that have found it difficult to cast a vote by traditional channels prior to the introduction of iVote® in the 2011 NSW State election.

With the implementation of an updated iVote® system for the 2015 State General Elections, NSW is again at the forefront of online voting worldwide.

Critics of online voting raise threats to the integrity of such systems from unauthorised access and manipulation. This Security Implementation Statement outlines how NSW Electoral Commission plans to secure the system and develop procedures to address perceived threats.

In support of this Statement, other documents provide greater detail of measures to ensure the iVote® system has the highest resistance to threats to its integrity. However, while this Statement is being published to support transparency of the iVote® system, not all security related documents will be made public.

I am particularly pleased with the introduction for 2015 of the ability of an elector using iVote® to verify their vote, which provides additional assurances of the integrity of electronic voting in NSW.

Colin Barry

NSW Electoral Commissioner

2 Executive Summary

The NSW Electoral Commission (NSWEC) will continue to develop Remote Electronic Voting (REV) using the iVote® system. This type of voting is allowed under NSW legislation for eligible voters for Parliamentary elections including the State General Election in 2015 (SGE 2015).

The use REV has been criticised both locally and abroad on the basis of risks to security and integrity of the system. However, the NSWEC has undertaken a comparative risk assessment to determine the suitability of the iVote® system for parliamentary elections, and has balanced security and community trust against the benefits REV brings both now and in the future.

The key security issues were identified from experience with the State General Election in 2011 (SGE 2011). The NSW Joint Standing Committee on Electoral Matters (JSCEM) made several recommendations related to iVote® which are being included in the 2015 implementation[1]. The principal recommendation related to security and trust was Recommendation 11 which said "…NSWEC develop and implement voter preference verification for voters using iVote® at the 2015 State election".

Eligibility to use the iVote® system is restricted to electors who are disabled, illiterate, live more than 20km from the nearest polling place or remote from NSW on election day. For SGE 2015, this cohort is expected to be approximately 200,000 voters. This restriction limits the risk of the system to the election as only a small subset of votes could be impacted by fraud or system failure. Furthermore, results of the traditional voting channels will be used to statistically verify plausibility of the iVote® result.

Importantly, the security of the iVote® system will include a mix of people, process and technology to provide a holistic system security and voting integrity approach.

Key features to increase community confidence in the iVote® system are:

- Voters can check their votes post-election.
- Independent auditors will review the iVote® system to provide assurance of its integrity and accuracy of and that the system operated as intended.
- The system's design and implementation will be reviewed by a team of experts with knowledge of electronic voting and information security.
- Testing the voting application will be undertaken at all stages in the project.
- Segregation of duty and access restrictions to legitimate business needs will ensure no individual has sufficient privileges to breach the system's integrity or voter's secrecy.
- Ongoing logging and monitoring of the system and user activities will ensure any potential threat to its integrity is quickly identified.

[1] Government Response to REPORT NO. 2/55, 2013, See Footnote 4
http://parliament.nsw.gov.au/prod/parlment/committee.nsf/0/129dfc87035dd10eca257ad10013144d/$FILE/Government%20Response%20-%20Administration%20of%20the%202011%20NSW%20Election%20and%20Related%20Matters.pdf

- Ongoing risk assessments of the changing threat landscape will enable additional mitigating security initiatives to be implemented.
- A range of appropriate information security controls will provide continued protection in the event that any single control is compromised.

3 Introduction

The NSWEC recognises the importance of security in Australian parliamentary elections and the integral part it plays in assuring the electorate that they can have confidence in our democracy. Security of all voting channels is paramount and each voting channel has its own unique challenges and security strengths. However, they are all part of the same system and the core security principles must be met.

The iVote® Remote Electronic Voting (REV) System was introduced for the State General Election (SGE) in March 2011 and has been used for subsequent state by-elections. Electronic voting (eVoting) uses electronic or computerised equipment to provide part or all of the vote-casting and vote-collection process. The enabling legislation for eVoting in NSW requires the implementation of a REV system. The NSWEC REV approach, as used in 2011, allowed voters to cast their vote using telephones or computers with browsers and Internet access. This approach was selected to meet the needs of the Blind and Low-Vision (BLV) community, which was the group of electors most active in advocating for the introduction of iVote® for the 2011 election[2].

As a result of the success of the iVote® system at the 2011 election[3], the NSW Joint Standing Committee on Electoral Matters (JSCEM) supported its use at the next SGE in 2015 following improvements related to transparency and voter confidence[4]. Notwithstanding the need to support BLV voters, legislation for the SGE in 2015 provides for the system to be used by remote electors, both those who live more than 20 km from a polling place and those that will be out of state on election day.

Significant research into electronic voting systems has been conducted over the past 10 years. Most of the research effort has been by computer scientists and has focused on developing voting technology capable of delivering proof the election outcome can be trusted[5]. Trust based on such a technology driven approach relies on the public either having a significant knowledge of cryptography or alternatively trusting someone who does.

It should also be noted that cryptographic proofs are of little use in improving the elector's trust at the point where the elector interfaces with the voting system. The human machine interface requires a different process to instil trust, such as a

[2] Report on the Feasibility of providing "iVote® " Remote Electronic Voting System, NSWEC 2010

http://www.elections.nsw.gov.au/__data/assets/pdf_file/0006/84498/20100723_NSWEC_iVote®_Feasibility_Report_.pdf

[3] Evaluation of technology assisted voting provided at the New South Wales State General Election, Allen Consulting Group Pty Ltd, March 2011

http://www.elections.nsw.gov.au/__data/assets/pdf_file/0004/93766/July_2011_Final_ACG_iVote®_Report_ELE01-C_Final.pdf

[4] ADMINISTRATION OF THE 2011 NSW ELECTION AND RELATED MATTERS, Joint Standing Committee on Electoral Matters REPORT 2/55 – DECEMBER 2012

http://parliament.nsw.gov.au/prod/parlment/committee.nsf/0/129dfc87035dd10eca257ad10013144d/$FILE/Report%202-55%20(Administration%20of%20the%202011%20NSW%20Election).pdf

[5] Verificatum is an implementation of a provably secure mix-net. Mix-nets are important components of electronic voting systems.

http://www.verificatum.org/

verification process where the elector confirms their vote has been captured as cast via information sent over an independent second channel. This approach to verification is considered by some researches to be unacceptable if the vote as cast is provided in the clear because it potentially allows the voter to be manipulated when voting.

Recommendation 12 of the Committee of Ministers of the Council of Europe (CoE)[6] states that manipulative influence should not be permitted, but in NSW for postal voting this risk is already accepted. Research in NSW[7] has shown that coercion or manipulation is not considered significant and the benefit of improved trust in the voting system through verification outweighs the need for greater coercion resistance.

The CoE recommendations[6] are generally considered the best high level benchmark for eVoting systems. Although CoE recommendations are not a security standard they comprise a comprehensive set of recommendations which if fully addressed give a high level of confidence in the security and integrity of the iVote® system. Compliance of the iVote® system with these recommendations is described in Appendix B.

[6] "Legal, Operational and Technical Standards for e-Voting", CoE Recommendation Rec(2004)11

http://www.coe.int/t/dgap/democracy/activities/ggis/e-voting/key_documents/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf

[7] Internet Voting and Voter Interference, Associate Professor Rodney Smith, Department of Government and International Relations, University of Sydney, March 2013.

http://www.elections.nsw.gov.au/__data/assets/pdf_file/0003/118380/NSWEC_2013_Report_V2.0.pdf

4 Scope

The scope of this document is to outline the security of the core components of the iVote® system – Core Voting System, Registration System and Verification System, along with the supporting people process and technology controls that make up the entirety of the system. As the iVote® system is only one of a number of voting channels, security aspects of the NSW SGE 2015 election as a whole will also be noted in this document to provide context for the security of the iVote® system.

The core scope of the document is for the use of the iVote® system in the SGE 2015, but will also include its subsequent use in future NSW by-elections, or use by other state governments and federal agencies that want to leverage the iVote® system for electronic voting.

5 Document Purpose

This document has been prepared by the NSW Electoral Commission (NSWEC) to provide an overview of the security strategy for the use of the NSW electronic voting system iVote® for the SGE 2015. Its purpose is to provide the public, electors and other interested stakeholders with information about the security principles, approach and controls that will be in place in respect of the iVote® system.

The objective of this document is to provide transparency in the formation of the iVote® system and to articulate that security has been at the forefront of the iVote® system design. This transparency aims to provide confidence in the iVote® system and the future use of electronic voting as a supplementary channel for voting in NSW elections.

The diagram below shows the overall structure of this document to assist with navigation.

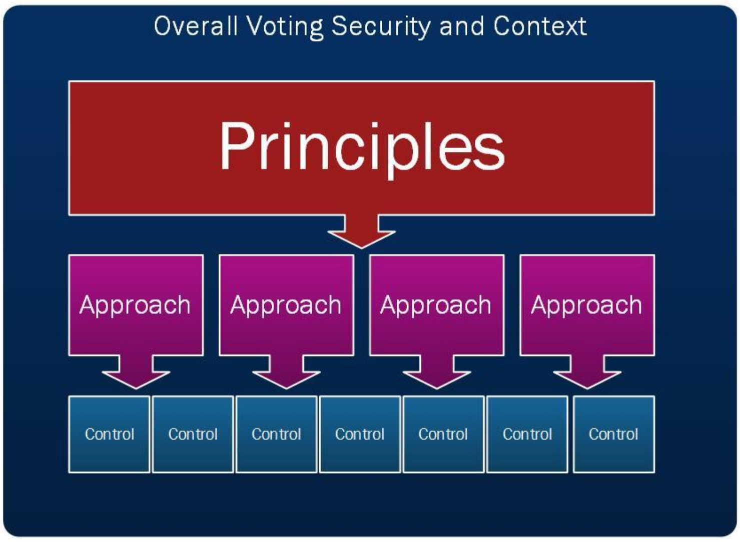


Figure 1 – Overall Document Structure

There are four main sections and each section contains the diagram above to illustrate how it is related to the rest of the document:

- Overall Voting Security and Context - describes how the iVote® system is planned for the NSWEC SGE 2015 and why security is important
- Principles - outlines the overall security objectives for iVote®
- Approach - describes the process taken to ensure iVote® has a high level of security in addressing the principles
- Controls - lists all the controls NSWEC has put or intends to put in place to manage the security risk for iVote®

6 Stakeholders

The following are the key stakeholders with an interest in the security and integrity of the iVote® system:

- NSW iVote® eligible voters – are the potential users of the iVote® system and therefore have direct contact with the system, and have the right to privacy and a secure voting process.
- NSW electors - electors must have confidence in iVote® as the iVote® system is one of the voting channels used in NSW parliamentary elections and contributes to the overall result of the election.
- Government – the government has enacted legislation requiring use of the iVote® system and has political, media and social responsibility for the result of the use of the iVote® system and any security incident that could arise.
- Political parties – the political parties rely on the NSW voting system to deliver an outcome that accurately reflects the voters' intent. Therefore, any security incident may have an effect on the confidence that the system has provided them with a fair election platform .
- NSWEC Commissioner – the Commissioner bears ultimate responsibility and accountability to run a successful election. As a component of the election delivery process, any security incident that affects the iVote® system may detract from perceptions of the overall success of the election.
- Technical Observers - Observers will form opinions based on available information about iVote® and will review these against their own perceptions and agenda. A lack of appropriate security measures or a security failure will be examined closely by this group.
- Media - The media will form opinions based on various facts, perceptions and issues around security for iVote®. Given the sensitivity that eVoting in general has in the eyes of the media, any security failure will be of interest to the media and hence might erode other stakeholder's confidence in the iVote® system.

7 iVote® Security Context

A holistic and methodical Cybersecurity approach has been taken to the implementation of the iVote® system and its use for the State General Election 2015. The iVote® security strategy is driven by principles of being comprehensible, and providing assurance in secrecy, integrity and availability. Security design for the iVote® system has benefited from local and global experience, in part provided by specialist third parties for specific expertise. Local experience was the successful use of remote electronic voting in the NSW SGE 2011 by 46,864 voters and by-elections since. NSWEC reviews reports on online voting activities by other jurisdictions globally and has been an official observer in international elections where electronic voting was used.

NSWEC is acutely aware of the security concerns surrounding the use of electronic voting both locally and global. These concerns have been addressed through the core design considerations, security principles, implementation and evaluation as part of an overall voting system.

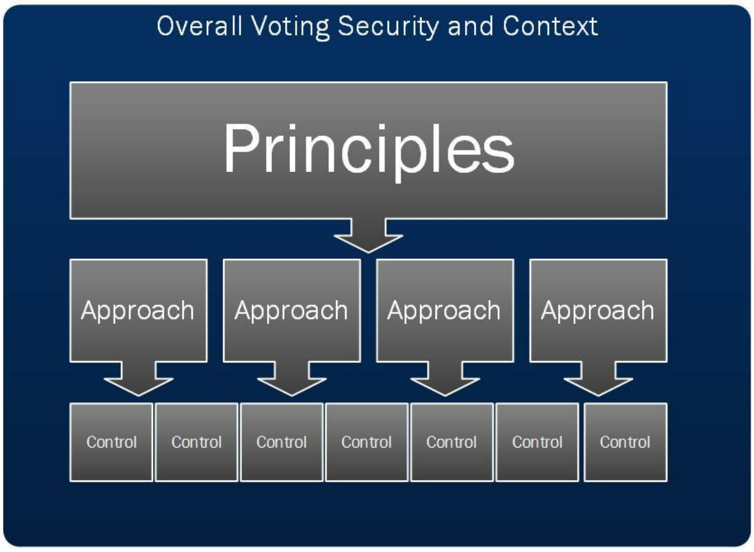


Figure 2 - Document Structure – Overall Voting Security and Context

The following diagram gives a conceptual overview of the iVote® infrastructure environment. The environment will include providing hosting support for the primary application components that form the iVote® system and associated functions required to operate the system effectively.

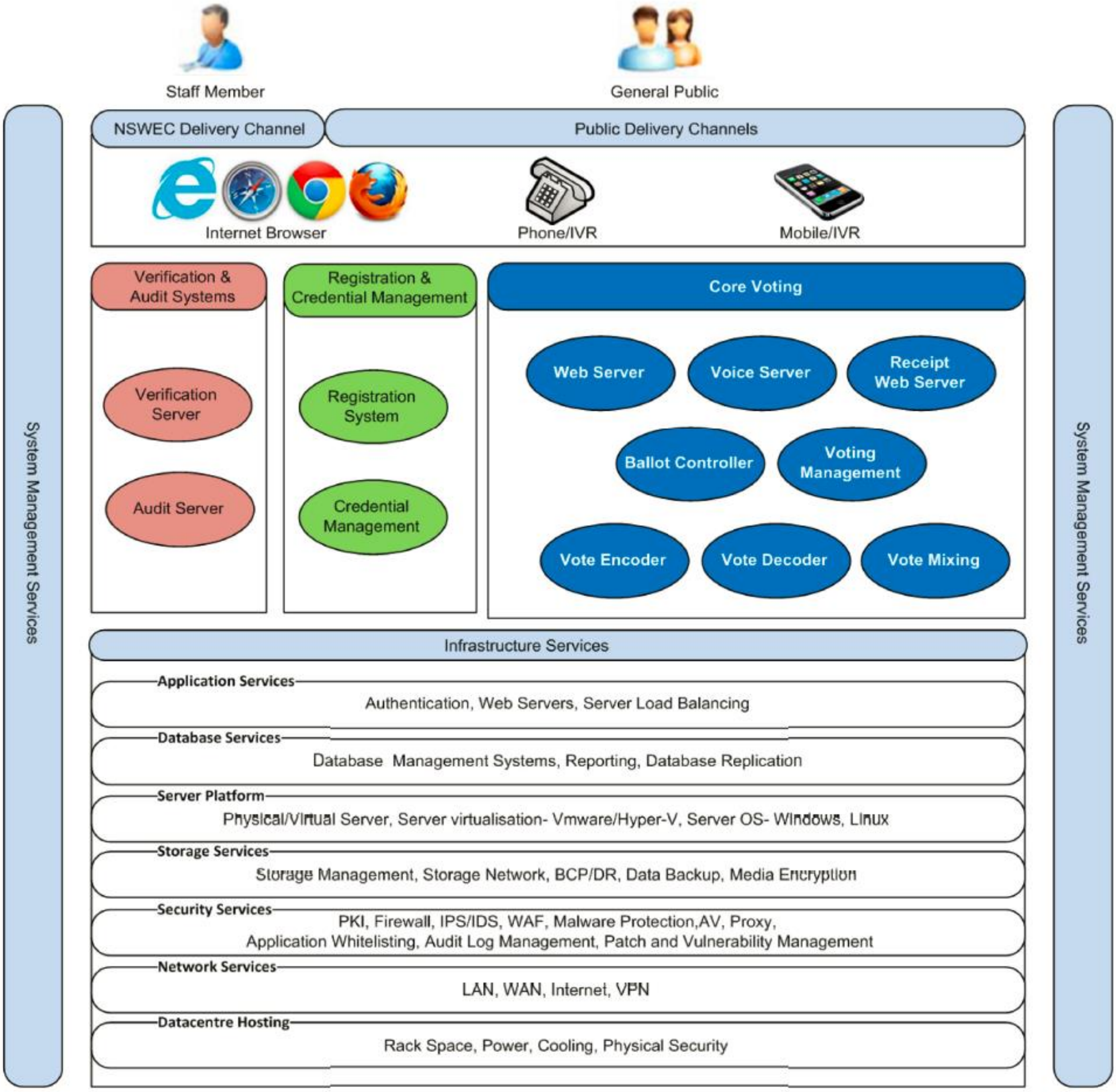

Staff Member
General Public
NSWEC Delivery Channel
Public Delivery Channels
Internet Browser
Phone/IVR
Mobile/IVR
Verification & Audit Systems
Verification Server
Audit Server
Registration & Credential Management
Registration System
Credential Management
Core Voting
Web Server
Voice Server
Receipt Web Server
Ballot Controller
Voting Management
Vote Encoder
Vote Decoder
Vote Mixing
Infrastructure Services
Application Services
Authentication, Web Servers, Server Load Balancing
Database Services
Database Management Systems, Reporting, Database Replication
Server Platform
Physical/Virtual Server, Server virtualisation- Vmware/Hyper-V, Server OS- Windows, Linux
Storage Services
Storage Management, Storage Network, BCP/DR, Data Backup, Media Encryption
Security Services
PKI, Firewall, IPS/IDS, WAF, Malware Protection,AV, Proxy, Application Whitelisting, Audit Log Management, Patch and Vulnerability Management
Network Services
LAN, WAN, Internet, VPN
Datacentre Hosting
Rack Space, Power, Cooling, Physical Security
System Management Services
System Management Services

Figure 3 – iVote® Conceptual Architecture

7.1 iVote® is not the main voting method

The iVote® system is an additional channel to the traditional voting system. The iVote® system will not replace paper ballots and under the current eligibility criteria is unlikely to comprise more than 5% of the votes cast for any one electoral contest. Overall for SGE 2015, an estimated 200,000 voters are expected to use the iVote® system

Because iVote® is only one of many channels, the results for iVote® can be compared with other voting channels which have similar electoral demographics. The lack of any substantial difference in the percentage of first preference results by candidate or group would eliminate any suspicion of tampering within the electronic voting channel.

7.2 Registration eligibility

In order to use the iVote® system the voter will have to register and meet at least one of the following eligibility criteria:

- reading difficulties,
- other disabilities,
- live more than 20km from a polling place, or
- are interstate or overseas on election day.

The criteria are contained in state legislation and are enforced through the registration processes. The restriction of iVote® usage means that only a limited number of voters are able to use iVote® which limits the potential impact of any security incident on the electoral outcome.

The registration process requires voters to identify themselves on the electoral by name, date of birth and enrolled address. In addition, the voter is invited to supply a driving licence or passport number. Where this additional authentication is supplied (thus providing greater assurance of identity than either postal voting or polling place procedures, it is considered the risk of voter impersonation is low. Where this information is not supplied, an acknowledgement letter is mailed to the voter's registered address. In any case where the voter has not registered (and therefore potentially impersonation has taken place) and contacts the registration call centre during the election period, the registration and any vote associated with it will be cancelled. The voter, if desired, can re-register to use the iVote® system. Re-registrations will also cater for cases where voting credentials have been lost or forgotten, or where coercion is alleged.

7.3 iVote® aligned with other early voting channels

The iVote® channel will run in parallel to the traditional early voting options of pre-poll and postal voting channels that will continue to be available in the SGE 2015. This will not only limit the timeframe for any exploitation or incident, but aligns with the comparative risks of the traditional voting channels.

This is achieved by:

- iVote® registration will commence at the same time as postal voter registration commences;

- iVote® voting will commence at the same time as pre-poll voting commences;
- iVote® registration will close at the same time as overseas pre-poll voting ceases;
- iVote® re-registrations will be allowed from the time pre-poll voting starts to 6pm EST on election day;
- Voting using the iVote® system at designated remote venues will occur from the traditional commencement of pre-poll to close of pre-poll for these venues; and
- The iVote® system will cease accepting votes at 6pm EST on election day.

7.4 Risk management comparison to traditional voting channels

The overall risks associated with the iVote® system will be commensurate with other forms of voting channels available to electors. The following table provides an assessment of the traditional voting system compared to the electronic voting system, and highlights some of the comparative security risks:

RISK	PAPER BALLOTS	ELECTRONIC VOTING
Impersonation	Using the current paper ballot approach potential voters only require a verbal declaration identifying themselves. The declaration requires them to know a name and address on the roll. Date of birth may be requested to ensure correct identification.	Similar to current paper ballot approach requirement but with option to provide additional identifying information such as driver's licence or passport number. Where this additional identifying information is not provided, an acknowledgement letter to their enrolled address will alert voter in case of impersonation.
Cast as intended	Elector can vote incorrectly causing their vote to be informal. General informality for paper ballots between 3% to 6%.	Guided to ensure vote complies with formality rules. Must make active decision to cast informal vote. Informality typically about 1%.
Captured* as Cast	Once the ballot paper is placed in the ballot box the voter must trust the Commission. Independent scrutiny is sporadic and mainly focused on polling place votes. The 30% of declaration votes are typically counted without independent scrutiny.	Voter can verify their vote has been captured correctly by checking the vote through the Verification Service. Even a small percentage of voters successfully verifying their votes will provide high probability of the integrity of the votes captured by the system.
Counted as Captured*	Trust the Commission staff manually counts the ballot papers correctly.	A receipt number website will publish all receipt numbers of votes included in the count. Published preference data, which is validated by auditors and electors, can be counted by anyone to check the count is correct. Compare to paper ballot results.
Tampering	It is difficult to identify evidence of vote tampering with paper ballots. Notwithstanding there is no evidence of this actually occurring in Australian elections.	Vote encrypted by voter's computer are not accessible by the Commission or others until decrypted. An independent auditor will check that decrypted votes are matched to votes on the Verification Service to ensure their validity. Electors can compare paper ballot results with

RISK	PAPER BALLOTS	ELECTRONIC VOTING
		electronic results which should have a very similar proportion of votes for candidates.
Ballot Box "Stuffing"	It is difficult to identify evidence of vote tampering with paper ballots.	Vote encrypted by voter's computer and not accessible by the Commission or others until decrypted. Decrypted votes matched to verified votes to ensure valid. Compare to paper ballots results.
Integrity	It is difficult to identify evidence of ballot papers which may have resulted from ballot box "stuffing".	Ongoing monitoring of registrations against votes would identify stuffing at time it occurs and potentially allow added papers to be identified and removed. Compare to paper ballots results.
Ballot Secrecy	Integrity of paper based elections relies on Commission staff following procedures and being trusted.	Combination of technology and procedures give the ability to be confident votes are counted as cast. Compare to paper ballots results.

* Captured - for paper ballots when placed in the ballot box or in a declaration envelope or for iVote® when the ballots are encrypted.

7.5 The iVote® system is not just technology - People / Process / Technology

NSWEC will implement the iVote® system not only as a technology, but as a system that is also based on people and process components of the solution, their interaction and inherent dependency as part of the iVote® system.

iVote® security is strongly reliant of its seamless integration with the traditional voting system and this is achieved through focus on the security of the people, processes and procedures of iVote® to ensure a holistic security solution.

7.6 Segregation of Duties and Data, Systems and Communication Channels

The iVote® system has been designed to provide security through segregation of duties, data and systems to achieve a defence in depth. Zoning and physical separation of the systems enhance the integrity of the overall system if one component is compromised. In addition, communication channels between the systems are restricted only to expected types of activity.

iVote® administrators have been segregated, both NSWEC staff and contractors, to provide separate core capabilities. Procedures will ensure no single contractor or administration staff member will have access or authority over the entire system, which provides further logical separation and largely eliminates complete system compromise without collusion amongst multiple parties. Furthermore, the system itself will be in "lock down" during the election period where only the Commissioner and the iVote® Manager have authority and ability to grant access.

7.7 Verification

Verification of votes is provided by the following:

- Independent verification service - At the time of voting, two copies of the encrypted vote are sent to the iVote® system, one to be placed in the virtual ballot box, and the other to an independent iVote® verification service. This service will be managed and operated independently from the rest of the iVote® system. A voter using the iVote® system will be able to access the verification service by phone via an Interactive Voice Response (IVR) system to verify that their vote has been captured correctly.
- Audit process - After the close of voting, the auditor will confirm that decrypted votes sent to the counting process are identical to those sent to the independent verification service. This provides assurance that integrity of processing of votes through the iVote® system has been maintained.
- Receipt number website - When voting using iVote®, electors are given a unique receipt number. After close of polls, the receipt numbers of all votes are decrypted revealing the receipt number and the vote which is included in the count. The receipt number is then sent to the receipt number website. Electors by entering their receipt number on the receipt number website will be able to confirm that their vote was included in the count, because it contains the receipt number they were given when voting.

7.8 Voter coercion not considered a significant issue

Australia has a strong democratic process and cultural history around secret ballots that include the principle that a vote can be made without coercion. There have been limited instances of voter coercion in the other traditional voting channels[7] and iVote® as another voting channel will not introduce any additional risk or opportunities to exploit than exist today.

The iVote® system has an anti-coercion mechanism in that it allows a user to re-vote during the voting period. At that point an elector could report any attempt at coercion which would be investigated as a criminal offense, as would alleged coercion in traditional voting channels.

7.9 Declining postal voting effectiveness

Postal voting is becoming increasingly problematic as an effective channel for remote voters. As use of postal services declines[8] in the face of digital alternatives, so will service levels of first class mail. It can be expected that future reduced postal service delivery schedules will challenge the feasibility of completing postal vote application, ballot distribution and return within election timetables to the point where, for many electors, postal voting ceases to be a viable voting channel.

[8] Australia Post chief says letter volumes "about to fall off a cliff", Post & Parcel, August 15th, 2014 http://postandparcel.info/62277/news/companies/australia-post-chief-says-letter-volumes-about-to-fall-off-a-cliff/

Declining postal service levels combine with much higher failure rates for postal compared to iVote® voting. In SGE 2011, for interstate and overseas voters only 3% of those registering for iVote® did not vote, compared to 25% of those applying for postal votes. For overseas postal voter applicants over 60% of postal votes not returned.

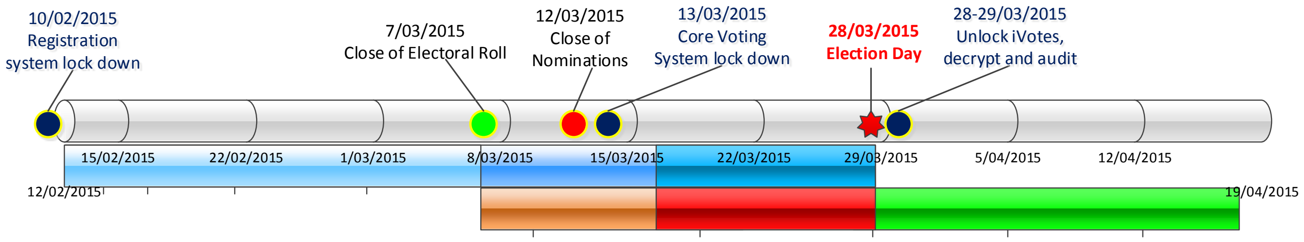
	POSTAL VOTES	iVote®
Did not vote at all	2,225	1,429
Applied to Vote	8,998	47,041
Failure Rate	**25.1%**	**3.0%**

Lastly, the secrecy of postal votes has been questioned in the courts due to nature of the required procedures to process the postal ballot. In order to process a postal vote an electoral official must identify the voter during preliminary scrutiny. To protect a voter's secrecy the electoral official must remove the vote from the envelope without seeing the preferences marked. Given most postal votes are opened without a scrutineer present or direct supervision it is likely that some election officials may be aware of how given electors voted. The iVote® system uses electronic means to separate the voter identification from the ballot which makes breaches of voter secrecy much more difficult.

7.10 Security by design

Security of the iVote® system has been at the forefront of the principles in the overall design of the system. Rather than adding auxiliary security controls to an existing system, NSWEC has built security in as part of the core requirements of the iVote® application and system. This is best demonstrated by the following security milestones and their relationship in the iVote® System Life Span:

NSW State Election Timeline and iVote System Life Span



NSW State General Election Major Events and Security Milestones

Prior – Extensive testing regime, including penetration testing

● 10/02/2015 – Registration system fully tested and locked-down for use

12/02/2015 – Pre registration (& re-registration) starts for remote voting.

● 07/03/2015 – Issue of writs, close of electoral roll and nomination starts.

● 12/03/2015 – Close of nominations.

Candidates loaded to iVote core voting system.

● iVote core voting system fully tested and locked-down for use

5 electoral board members secure virtual ballot boxes.

'Logic and Accuracy' testing performed with test votes decrypted

16/03/2015 – pre poll & iVote voting starts and registrations continue.

✶ 28/03/2015 – iVote re-registration, election day & iVote voting ends @6pm,

● Quorum of electoral board members open iVote virtual ballot box.

Decrypted votes for the count are independently re-encrypted and matched to the encrypted votes from the Verification service to confirm no tampering.

29/03/2015 – Load LA & LC preferences to PRCC for counting.

02/05/2015 – Return of Writs.

🟦	Pre registration & re-registration – Remote
🟦	Registration & re-registration – Remote
🟦	Registration & re-registration – Remote and Remote Venue
🟧	Core voting system configured and go live period
🟥	iVote Pre poll voting and election day voting
🟩	Audit & open virtual ballot box

8 Principles of iVote® Security

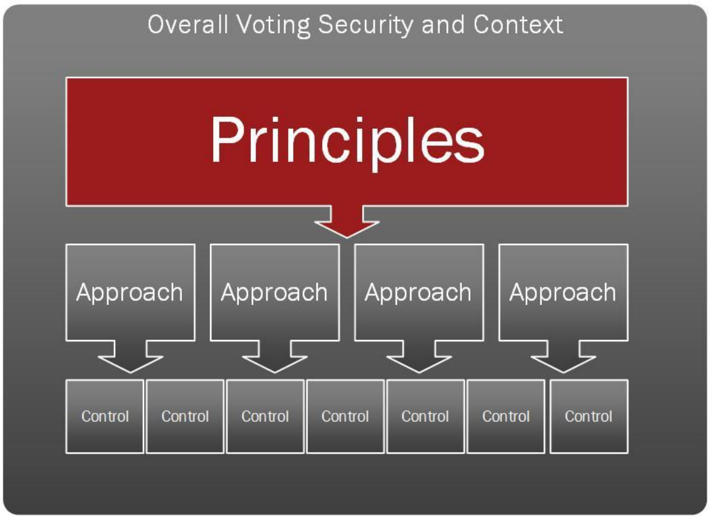


Figure 4 - Document Structure - Principles

In the context of iVote® and voting, the adopted security strategy need to generate strong confidence in the system from all stakeholders, whilst also providing an appropriate level of transparency. Therefore, the following are the core principles which have driven the iVote® security strategy.

8.1 Comprehensible

Due to the public nature of elections, iVote® security must be able to be understood at some level by the average voter. The security design, principles and the reasons for the implemented controls must be clear and have meaning to the electorate. This includes comprehensible language and explanations that cover the people, processes and technology controls used in the iVote® system to provide confidence and transparency.

During the iVote® project, the NSWEC has published (and will continue to do so) key documents. Additionally, specific documents and briefings have been provided to NSW parliamentary bodies to support their governance role in all electoral matters.

8.2 Secrecy

A feature of electoral environments in western democracies is that an elector's vote is secret and therefore the elector should also not be able to prove how he/she voted to any other person. There are two aspects to secrecy for iVote®: that

- the system cannot identify how a person voted;
- when a person votes remotely they can do that in relatively privacy and in secrecy, or with the assistance of whoever they nominate, free from physical observation.

Addressing the first point, the iVote® system has been designed to ensure the electoral authority can never know how a given elector voted. This is achieved by the system removing the elector identifier from the vote as cast prior to the vote being decoded.

In respect of the second point, physical secrecy for REV risk is no different to postal voting where voting takes place at a location outside the control of NSWEC.

8.3 Integrity

Integrity of the iVote® system is achieved through technology by design, assessment, monitoring and audit. Technical approaches to maintaining integrity include all reasonable measures to resist threats.

It is impossible to absolutely guarantee that a system cannot be breached. However, should a breach occur, continual monitoring of application and system parameters across all components iVote system will ensure that any unexpected activity is detected as soon as possible so that remedial action can be taken.

The impact of any breach will be limited by separation of systems and data, so that two systems would need to be compromised undetected in order for any votes to be manipulated or privacy to be at risk.

Processes and procedures have been designed to ensure the people component of the iVote® system, complements the technology. These include a requirement for all manual processes (for example configuring the system in preparation for an election) require an operator and observer who both sign a record of the steps completed. Such procedures ensure integrity by preventing any undetected or authorised actions that could override the technology of the system.

In addition, at close of poll, scrutineers and auditors will check that the votes captured and decrypted match those held in the Verification Service to provide the assurance of overall integrity of the iVote® system.

8.4 Availability

The system is designed to provide the required availability during the period of the election. Security will contribute to availability through controls implemented that will protect the system from attacks intended to cause an outage. Typical Cyber-attacks that focus on the outage of a system are Denial of Service attacks and malicious software that may affect the usability of the application or platforms.

NSWEC has designed and implemented security controls to contribute to the overall availability of iVote® during the election period, which is complemented by a disaster recovery strategy involving backup hosting sites for all iVote components.

9 Approach to address Security Principles

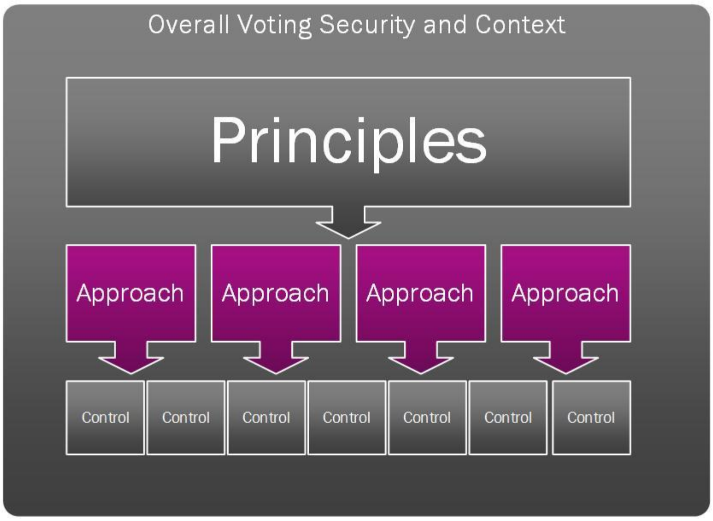


Figure 5 - Document Structure - Approach

The following section describes the various inputs to implementing the principles, under which the security controls have been designed.

9.1 Lessons learnt

An independent auditor conducted a post implementation review of the iVote® system as used in SGE 2011. The purpose of this audit was to confirm that the security, accuracy and secrecy of the votes taken by the system were maintained.

9.1.1 Risks identified

Constraints from NSW SGE 2011 included a tight implementation timeframe due to the late passing of the enabling legislation. As a result documentation was incomplete and there was limited testing, although it was concluded by the auditor that the iVote® system's implementation was successful. However, the auditor did list out the risks that should be actioned for redevelopment. The issues raised were testing of all applications, incomplete documentation for iVote® and no Intrusion Protection System (IPS). NSWEC has assessed these risks and have addressed them for the SGE 2015. Furthermore, NSWEC has started planning for iVote® use in SGE 2015 well before the election to allow sufficient time for adequate design, implementation and testing.

9.1.2 Non-Security Incidents

Five incidents during NSW SGE 2011 were determined to have in no way affected the security or secrecy of the votes and were not material to the electoral outcome. They could however have affected the electorate's overall perception and confidence in the system.

These incidents were:

- Some electors received seven digit iVote® numbers (instead of eight). Affecting the iVote® principle of assurance
- A reminder was sent to people who had already voted in iVote®. Affecting the iVote® principle of assurance
- A short failure of the inter-site link between iVote® data centres (an alternative link ensured no actual interruption). Affecting the iVote® principle of availability
- Short outage of live iVote® system (approx. 8 mins). Affecting the iVote® principle of availability
- iVote® by web allowing the letter "N" onto 43 ballots. Affecting the iVote® principle of assurance and integrity

These incidents were analysed and formed part of the NSWEC iVote® knowledge base for future REV development. NSWEC will implement thorough functional testing for iVote® use in SGE 2015, and has also included security testing even though no such issues occurred during the SGE 2011.

9.1.3 Submissions to JSCEM

Post SGE 2011, the NSW Government gave the Joint Standing Committee on Electoral Matters terms of reference to review the election. The review reports[1,4] support the ongoing use of iVote® but identified two main issues for NSWEC to consider for subsequent elections. The first was the need for greater transparency, while the second was the need for the elector to be able to verify their vote as cast.

Redevelopment

Based on the information received post NSW SGE 2011 iVote® will be implemented for NSW SGE 2015 with improvements to transparency and integrity of the iVote® service, public awareness and confidence in the iVote® service and vote verification - that votes, as cast, were included in the count.

Mitigation of Risks

To ensure the risks identified from NSW SGE 2011 are managed in the redevelopment of the iVote® system additional controls will be imbedded in the development phase that include quality assurance and testing processes, system security, risk management, systems audit.

9.2 International electronic voting experience

Design of the iVote® system and its implementation has also taken into consideration remote electronic voting implementation, challenges faced and incidents experienced by jurisdictions overseas.

Well documented incidents include:

- Washington trial where computer experts were encouraged to attack the system, which resulted in the trial being suspended due to security risks being identified;
- breach of the Florida voting database in 2011 in order to demonstrate that voting fraud can easily happen; and

- Anonymous – in the Ohio 2012 election it was claimed they stopped voter fraud by putting up firewalls to stop the votes being manipulated.

There were also minor issues noted with the Norwegian elections 12 votes were lost in their first election, and during their second there was an error with the random number generator.

NSWEC has been invited as observers by overseas governments in respect to use of remote electronic voting in their elections. This experience and the lessons learnt from the international incidents have been used in the overall design of the iVote® system to overcome most of the issues identified above.

9.3 Design

Using the lessons learnt from SGE 2011, NSWEC has improved the design, overall implementation, and third party involvement for SGE 2015.

As a starting point for SGE 2015,A strategy document was published on the NSWEC website two years before the election. The document was used to support funding submissions and to garner public support and feedback.

Tenders for major iVote® components were published, principally the Core Voting System (CVS) CVS Hosting and Verification Service. Details of each of the systems, the architecture, software and hardware specifications; and voting protocols and principles under which the iVote® system will be implemented were included in tender documentation.

The underlying design objectives for iVote® are to ensure voter secrecy and security, and integrity of the registration and voting process. Key to the design is that multiple systems would need to be breached to affect any one of the core security principles. The system ensures a given elector’s identity and vote spans at least two systems and is encoded in both systems. Consequently, a breach of vote secrecy could only occur if system breaches occurred and the encryption was broken.

The iVote® system has been designed to ensure minimal risk of vote tampering occurring without detection. It would require access to the core voting system without leaving any trace because such access is restricted during voting and all actions in the system are held in immutable logs.

iVote® for SGE 2015 has been designed to provide improved audit and security monitoring of the system. Other improvements include updated processes and procedures that integrate with the system design.

9.4 Threat Analysis

NSWEC identified from the previous project that it is not feasible to deal with all security issues equally. It was therefore decided that iVote® risks should be assessed on a threat basis. Threat analysis to identify key threats was undertaken by an independent party as a foundation for a proactive security strategy. As threats continue to evolve, specific threats need to be monitored on an ongoing basis to determine status changes.

This analysis was on the basis of the systems architecture and implementation procedures proposed in the iVote® strategy document. An initial analysis was conducted of threats and risks associated with provision of iVote® services for SGE

2015, including both the proposed iVote® technical platform and procedures associated with operations for SGE 2015 using an attack tree approach and desktop exercise to exhaust each attack possibility and test defensive measures.

This process was conducted in two phases. The first part consisted of documenting the major threat actors that threaten iVote® for SGE 2015. They were then mapped to attack trees relevant to those actors. In the second phase exposures were then identified that might exist from the attack trees. From this, a course of action and threat analysis report was compiled.

Recommendations were made for NSWEC to consider for the design of iVote®. These recommendations included considerations for people, processes and technology for the redevelopment project.

The following are a summary of the core recommendations that are detailed within the report:

- Protection of the application and system during development against any malicious code.
- Ensure the integrity of the audit and logging systems by testing expected outputs, correlation and time stamps.
- Establish strong DDoS (Distributed Denial of Service) protection and countermeasures.
- Implement additional security controls on the registration system and associated database.
- Conduct security awareness training for staff, contractors and voters.
- Continued and accelerated threat actor monitoring leading up the SGE 2015 for any changes in capability, intent or triggers that may be a catalyst for an attack.

NSWEC have taken these recommendations into consideration when designing the redevelopment of iVote® system and the implementation and roll out of the system.

9.5 Security Risk Analysis and Management

NSWEC has a structured approach to risk management, which is being applied to the iVote® project. In addition to the internal processes of risk assessment and management, NSWEC has also contracted third parties to conduct reviews and risk assessments in order to determine whether the iVote® system is suitable for live operation and meets the security principles.

9.5.1 Threat and Risk Analysis

The threat analysis report provided by an independent third party resulted in the integration of threat attack vectors into the solution via risk management. Controls will be implemented to mitigate identified risks where possible. These will include both a technical and non-technical approach – people, process and technology. The security controls will contribute to the core security principles.

9.5.2 Analysis of the iVote® Protocol

Independent expert consultants have evaluated the completeness and appropriateness of the technical voting solution by analysing documentation on the iVote® protocol and requirements and specifically the architecture, functional and non-functional requirements described in Attachments A1, A2 and A6 to the CVS contract. NSWEC has updated the risk register and also the design of the solution in order to remediate or mitigate identified issues during several reviews.

9.5.3 Technical Risk Assessment

A technical security review was conducted of the iVote® architecture and controls. This included the identification of standards and frameworks for which the application will be audited against; and a security threat mitigation assessment to identify threats as well as a gap analysis assessment to support further risks reduction.

9.6 Assurance in iVote® development process

Assurance during the iVote® development process ensures errors are prevented and the iVote® system meets the functionality and objectives outlined. Quality assurance standards or other documents will be used to examine and test the application logic. These documents include standards for logical diagrams, program documentation, test planning, and test data acquisition and reporting.

9.6.1 Advisory groups

NSWEC has engaged specialised consultative groups to provide review, strategic guidance and advice. They include a Technical Advisory Group of international online voting and security experts and a Stakeholder Reference Group including representation of blind/low vision and disabled constituencies. These groups have various roles later discussed in the controls element of this document, but each group may also review security within their terms of reference.

9.6.2 Secure Software Development Life Cycle (S-SDLC)

The iVote® Core Voting System has been developed using an S-SDLC methodology to ensure that the security requirements are assessed and incorporated at every step of the development process, from analysis through to testing and production.

9.6.3 Readiness testing

Before iVote® goes live for each election, testing will be conducted to ensure it will perform as expected and the security principles are met. For the initial use of the system at the SGE 2015, this will include testing of required functions, the set of supported devices, browsers and operating systems (PC, tablets, smartphones), end-to-end processes and a formal election simulation as part of a system audit prior to lockdown. Together with the lockdown process, file signing, file integrity monitoring and pre- and post- election audits, this testing confirms that the live system used for the election is identical to the implementation tested and that no changes have been made to the system during the lockdown period.

9.6.4 Meeting industry standards

The voting system will comply with the following standards where applicable:

- AS/NZS ISO 9001:2008 Quality management systems -- Requirements
- AS/NZS ISO/IEC 27001:2006 Information technology - Security techniques - Information security management systems - Requirements

- Australian Government Information Security Manual (ISM)[9]
- ISO/IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM)
- ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
- ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components
- ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components
- Secure Development Lifecycle (BSIMM/OpenSAMM)
- CERT Secure Coding[10]
- FIPS 140-2, Security Requirements for Cryptographic Modules
- NIST Computer Security Division's (CSD) Security Technology Group (STG Cryptographic Toolkit[11]
- FIPS 180-4: (2012): Secure Hash Standard (SHS)
- FIPS 186-4: (2013): Digital Signature Standard (DSS)
- FIPS 197: (2001): Advanced Encryption Standard (AES)
- FIPS 198-1: (2008): The Keyed-Hash Message Authentication Code (HMAC)
- RSA Laboratories - Public-Key Cryptography Standards (PKCS)
- NIST SP 800-133, Dec-12, Recommendation for Cryptographic Key Generation
- NIST SP 800-130, Aug-13, A Framework for Designing Cryptographic Key Management Systems
- NIST SP 800-128, Aug-11, Guide for Security-Focused Configuration Management of Information Systems
- NIST SP 800-115, Sep-08, Technical Guide to Information Security Testing and Assessment
- NIST SP 800-108, Oct-09, Recommendation for Key Derivation Using Pseudorandom Functions
- NIST SP 800-107 Rev. 1, Aug-12, Recommendation for Applications Using Approved Hash Algorithms
- NIST SP 800-106, Feb-09, Randomized Hashing for Digital Signatures
- NIST SP 800-67 Rev. 1, Jan-12, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

[9] http://www.asd.gov.au/infosec/ism/index.htm

[10] http://www.cert.org/secure-coding/

[11] http://csrc.nist.gov/groups/ST/toolkit/index.html

- NIST SP 800-64 Rev. 2, Oct-08, Security Considerations in the System Development Life Cycle
- NIST SP 800-57 Part 1, Jul-12, Recommendation for Key Management: Part 1: General (Revision 3)
- NIST SP 800-57 Part 2, Aug-05, Recommendation for Key Management: Part 2: Best Practices for Key Management Organization
- NIST SP 800-57 Part 3, Dec-09, Recommendation for Key Management, Part 3 Application-Specific Key Management Guidance
- NIST SP 800-44 Version 2, Sep-07, Guidelines on Securing Public Web Servers

This provides assurance of the system from a security perspective by compliance with these well-known industry frameworks and national government standards.

9.7 Community awareness

NSWEC will ensure the community is aware of iVote® and its use, including that iVote® meets the security principles and that the risks in comparison to voting through other channels, such as in-person or by post, are either favourable or no greater when using the iVote® system.

NSWEC will implement a public information and education campaign prior to iVote® going live, which will also ensure that eligible electors are aware of the security and secrecy features of the iVote® system. As part of the transparency of the iVote® project, this Security Implementation Statement will be published on the NSWEC website to provide security information to electors and the general public.

During the iVote® voting period, several active support services for electors and specific community groups will be available. For example, Vision Australia and Blind Citizens Australia will ensure electors with impaired vision are informed of iVote® and its accessibility for them.

After the election, NSWEC will conduct a survey of electronic voters, including those who registered for iVote®, but then did not use it. The survey will, amongst other issues, assess trust in the iVote® system.

In addition, to provide transparency to the community, the source code of iVote® will be available to organisations or individuals who are willing to work within the NSWEC terms of engagement and have appropriate skills and knowledge to assess the system meets stated specifications or reasonable community expectations and results of such reviews will be published on NSWEC’s website.

9.8 Assurance during election period

During the election period a number of activities will provide assurance to the stakeholders that the system meets specified requirements. This includes:

Lockdown

The iVote® Systems will be “locked down” prior to the commencement of voting and managed in such manner that only the Commissioner and iVote® Manager will have the credentials and ability to access the system. All other staff, contractors and third party suppliers will have only the minimum, defined access, if any, to the system as necessary for the functions that they are required to perform. The lockdown deployed at multiple layers within the technology stack and in particular operates at the server, router and firewall levels to prevent any change to the iVote® system.

Cryptographic Keys

An Election Board is formed to generate the election keys, which are a pair of asymmetric keys, one public and one private. This board will comprise at least 5 members and a set minimum quorum of members, e.g. three of the five, is necessary to reconstruct the private key.

The public key is loaded to the vote encoder for the encryption of votes, while the private key is only ever used on an offline computer (not connected to any network) within the physical control and security of NSWEC.

Using asymmetric cryptography ensures that the encrypted votes cannot be accessed on the iVote® servers because, while the public key is used for encrypting the votes, only the private key is able to decrypt the votes.

Encryption of the votes is done in the browser of the voter (in the case of telephone voting this happens on the server), so the privacy of a voter’s preferences are not vulnerable to man-in-the-middle attacks, or attacks on the server.

Testing

The NSWEC may cast dummy votes using unique preference patterns during the live election to demonstrate that the voting system is working as intended and no security flaws are evident or that the system has been compromised. The votes cast will be indistinguishable by the system from any other vote and each will be manually removed prior to the votes being passed to the counting system.

Registration Call Centre

The primary iVote® call centre will accept registrations for iVote® and will also provide first-level support for electors in regards to iVote®, whether the enquiry concerns eligibility for iVote® or difficulties in actually voting.

Voters will have the option to re-register and re-vote by contacting the registration call centre. This is primarily available for electors who have forgotten their PIN, but will also limit voter coercion.

Voting Call Centre

Voters have the option to vote through a call centre operator (note that this call centre is separate from the Registration Call Centre where the identity of the elector calling may be known). For all votes taken this way simultaneously recordings of are made of both the screen of the operator and the voice call with the voter. To be able to vote, the elector only provides the operator their iVote® credentials (iVote® Number and PIN) and not their name or other personal details. The operator cannot find their name from their credentials so the voter’s vote remains secret. The recorded voice and corresponding screen activity is then reviewed by a separate operator who deletes the recording after the vote cast is confirmed to be exactly as per the instructions from the elector.

Verification Vote Checking

Each new vote created in a browser is duplicated then encrypted using the ElGamal encryption system. Both votes are then sent to the iVote® server, which places one in the ballot box and the other is transferred to the separate server of the Verification Service. ElGamal, due to its homomorphic properties, allows a zero knowledge proof of these votes to be done when they arrive at the iVote® server. This gives confidence that the votes have not been tampered with during transmission.

Elector Verification

Voters will be able to verify that the votes held in the Verification Service are recorded as the voter intended. This is done by voters phoning the Verification Service IVR system and being read out the preferences of their vote as captured. This then allows them to decide if the vote captured was the vote they intended to cast. If not then they can cast another vote (by calling the contact centre to re-register), and the original vote is cancelled.

This verification process protects against attacks that take over the browser or computer of the voter, through virus or other malware. It is preferable that the call is not made from the same smartphone used to cast the vote as there has been evidence of malware affecting Android phones, and possibly jail-broken iPhones, which can change the behaviour of the device when making or receiving calls or SMS messages.

A voter can call anytime between casting their vote and the close of the election and can call more than once to confirm that their vote in the Verification Service is as they cast it and no tampering has occurred.

Auditing Verification

Independent ‘auditors’ will confirm that the votes held in the Verification Service are the same as votes decrypted for counting. This is achieved by several independent teams re-encrypting the decrypted votes from the core voting system and comparing them to the votes held on the verification server. The process will be done under scrutiny of observers and the auditor will declare the process complete when either all participants agree the votes match or issue a finding.

The verification process provides assurance that the pool of votes in the verification server correctly represents the votes as cast by voters, even if only a sample of the total votes are verified, since any attacker could not know which votes would be verified.

The independent confirmation that the pool of votes in the verification server matches the votes from the core voting system (as sent to the counting system) provides strong assurance that there has been no vote tampering. There is full separation between the verification system and the core voting system, with separate hosting in different physical data centres provided by different commercial organisations, running software provided separately by two other, separate organisations.

Monitoring and Logging

All components of the iVote® system will include full logging and monitoring of all relevant system activities and configuration changes. These logs will be immutable and collected by a separate logging server. The logs will not contain information which allows a vote’s preferences to be explicitly associated with a given voter. Monitoring and logging will help NSWEC identify security breaches like hacking attempts, virus or worm infections as well as investigate configuration problems, exploits, and hardware problems.

Positive Media Coverage

The media will play a large part in the successful adoption and acceptance of iVote®. Voting is very personal and very public and the media provide extensive coverage on elections and tend to sensationalise stories. As iVote® is a channel of voting any negative coverage could create a perceived loss of confidence in the system. On the other hand, positive coverage would actively promote the use of iVote®.

NSWEC will provide its senior leadership to answer media questions on the subject and also actively participate in industry and stakeholder forums to encourage positive media coverage of the iVote® system. This will provide a successful platform for the positive coverage of iVote® and hence increased assurance and confidence in the system.

Successful management of the iVote® project will also play a key role in ensuring positive media coverage, both through the avoidance of any major incidents, which would cause negative media coverage, and also through the application of the principal of transparency, by providing appropriate details of the iVote® system to the public, auditors, technical reviewers, etc.

9.9 Monitoring and Security Incident Response

9.9.1 Security Monitoring

The security monitoring of the iVote® system will be covered in a multi-tiered in-depth defence strategy that covers people, process and technology. A tier 1 Security Operations Centre provider will be employed to collect, correlate and analyse technical security event logs as well as integrate into a threat management system providing near real-time event analysis.

In addition, the NSWEC service desk will provide security monitoring based on direct voter feedback for any cases of subversion, coercion, or error that maybe a result of a security breach.

Lastly, the third-party auditor will be monitoring the audit systems and will also investigate in the event of a security incident.

9.9.2 Security Incident Response Plan

Comprehensive logging and real-time monitoring will assist in early detection of security incidents. Security Incident Response includes the preparation and planning for a security event as well as the response itself. The response takes the form of the integration of the detection, analysis, mitigation and resolution to an event.

9.10 Audit

Independent audit of the system is a key feature that will occur before the system is live, during the operation of the system and post-system. The audit reports are provided to the NSWEC for public disclosure.

Pre Implementation

A pre-implementation audit is conducted by an independent auditor who reviews the implementation and operation of the system and provides recommendations on how to reduce or eliminate risks that could affect the security, accuracy or secrecy of voting. The auditor's role includes the review of security testing, including penetration testing of the iVote® system, and reviews of expert analysis of the source-code, of the cryptography and of the infrastructure.

iVote® Period

During the voting period the independent auditors will have access to the logging and monitoring, as collected by the Security Operations Centre, and will be able to verify that no tampering is evident with the data or the software comprising the iVote® system.

At the close of the voting period, the auditor will confirm that the votes held in the verification system are the same as votes counted. This verifies there has been no vote tampering as the vote passes through the iVote® system.

Post-Election

A post-election audit report will be completed by the independent auditor. The auditor will assess the overall accuracy, completeness and security of the iVote® system in regards to its use for the election event.

10 Controls

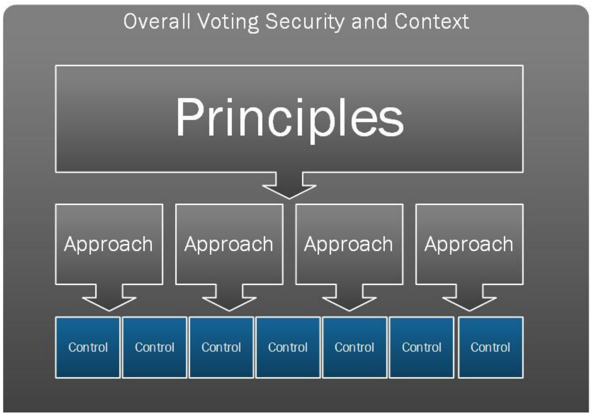


Figure 6 – Document Structure - Controls

In order address the security principles and taking in to consideration the security approach to the iVote® solution the controls have been designed to be integrated, complimentary and ultimately meet the objectives. Section 11 of this document maps these controls back to the security principles.

The controls address security from a holistic perspective including the security attributes that people; process and technology integrate to provide an end to end security solution.

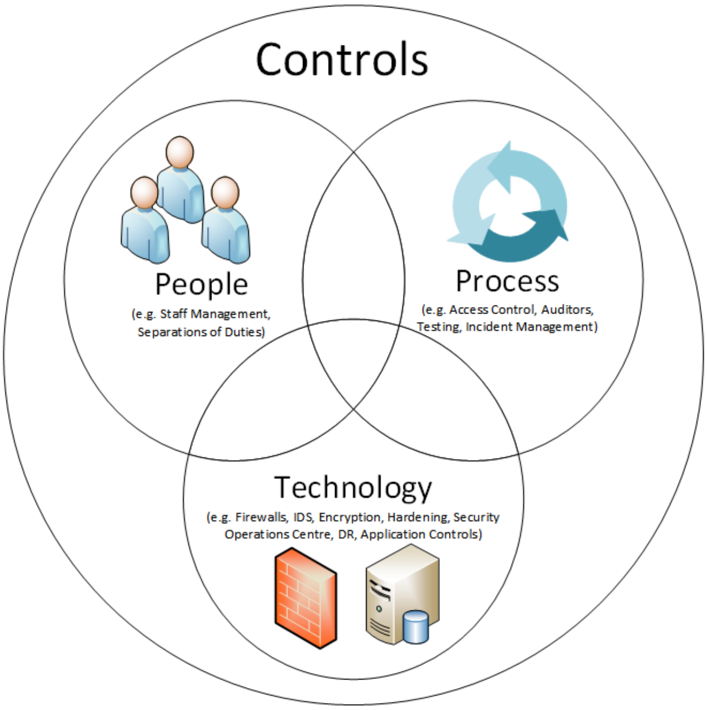

Controls
People
(e.g. Staff Management, Separations of Duties)
Process
(e.g. Access Control, Auditors, Testing, Incident Management)
Technology
(e.g. Firewalls, IDS, Encryption, Hardening, Security Operations Centre, DR, Application Controls)

Figure 7 – iVote® Controls

10.1 People

People are an important component of the security system. They can have the ability to override the process or technology security controls in place, depending on their interaction with the system and level of access. The traditional forms of voting also heavily rely on people in order to manage the election, count and publish the results – this system has evolved and been trusted since the inception of Australia’s democracy. Hence it is natural that people also play an integral part in the iVote® system to provide assurance of the voting system.

10.1.1 Staff Management

NSWEC is a statutory body responsible for running NSW State elections and has extensive experience managing staff for running successful elections. NSWEC follows NSW State Government policies in regards to staff management, with additional requirements for all staff to make a political neutrality statement.

During the staging of a state-wide general election, NSWEC hires over 20,000 temporary staff, primarily as polling place officials at the 2,700 polling places.

10.1.2 Election Specific Employment

As in the traditional voting system, NSWEC may hire staff specifically for the election to assist with the management of iVote®. These personnel will undergo character assessment to ensure their background will not affect the security of iVote®. They will also be checked to ensure they are in no way affiliated with a political party, threat actor or have any conflict of interest.

10.1.3 Clear Roles and Responsibilities

All people involved with the delivery of iVote® , whether permanent or casual staff, contractors or suppliers will have a clear definition and understanding of their role, function and responsibilities. There will be security responsibilities for all employees across the organisation involved in the NSW SGE 2015 and iVote® , and these will be outlined in the process and procedures documentation.

10.1.4 Separation of Duties

There will be segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system. The roles and their associated privileges are defined and documented. This will contribute to the overall security of the iVote® system and importantly link into the roles and responsibilities.

10.1.5 iVote® Manager

The Commissioner will appoint a person to be the iVote® Manager who will be his delegate to manage the iVote® system for the election. Although other key staff will support the iVote® manager, the direct management and security of the system will be the responsibility of the iVote® manager. Certain key steps will require the action of both the iVote® Manager and the Commissioner together, since the Commissioner holds ultimate accountability.

10.1.6 Security Awareness and Training

As a complement to the technical controls in place, a high degree of security awareness amongst the NSWEC iVote® team, call centre operators and third party contractors involved in managing the system during the election period will facilitate quick identification and escalation of unexpected system behaviour. To build this awareness, a range of information and activities will include the following:

- FAQs for electors using the iVote® system, demonstration iVote® system including IVR
- Training for call centre staff on their roles and potential anomalies in iVote behaviour
- User guides and training on security monitoring and escalation processes for those monitoring the iVote® Splunk dashboards and interfacing to the CSC Security Operations Centre.

10.1.7 Stakeholder Groups

The involvement of planned stakeholder consultative groups will provide review, strategic guidance and advice, as well as provide a security review of their components. They will include:

Technical Advisory Group

Membership to the group will be by NSWEC invitation on the basis of expertise and ability to make a contribution to the design and implementation of iVote®. This will include a security review function of the iVote® system including its principles and the ultimate security controls in place.

Stakeholder Reference Group

Membership to be by invitation of the NSWEC, based on involvement with aging, disabled, vision-impaired and other target elector categories, and ability to make a contribution to understanding the requirements of these stakeholders. This group will specifically provide advice on security, training and awareness, relevant to the targeted elector groups.

10.2 Processes

A process is a series of actions or steps taken in order to help secure iVote®. These processes involve people and procedures in order to help minimise the risk and provide a holistic and integrated security for iVote®.

10.2.1 Systems Access Control

Access controls are a key security element in order to provide a secure system.

iVote® Systems Access

NSWEC will limit and control access to protect the iVote® system and data integrity. Tools used to control access will include user-name and password, digital signing and use of certificates issued by a certificate authority owned by or acceptable to NSWEC. Only authorised individuals will be allowed access to any election data.

Dual Authorised Access

The iVote® procedures will require that at least two authorised election officials witness all manual tasks performed on the system that could influence the outcome of the election.

Infrastructure Lockdown

iVote® systems will be “locked down” and managed in such a manner that only the Commissioner and iVote® Manager will have the ability to access the system during the election period. The lock-down will occur prior to the election period when an approved version of the iVote® software is installed and configured, and as soon as the final testing is complete. This will only be done after iVote® has been independently verified.

Ballot Box/Election Keys

The electronic ballot box is secured by the election keys which will be held by five trusted people, with a quorum of three required to open the ballot box. Such a control reduces the risk of a single person acting in error or nefariously and reduces collusion and coercion risks by increasing the number of staff required to enact the ballot box opening.

Administration Keys

Cryptographic keys will be created by an Administration Board, similar, but smaller than the Election Board. The keys will be used to cryptographically sign key elements, for example the election configuration file, which will allow the signatures to be checked to prove that the signed data has not been altered since signing. A minimum of two of the Administration Board members would be required to create a valid signature.

10.2.2 Integrity Checks

Scrutineers

Appointed scrutineers can have supervised access to relevant elements of the election using iVote® between the issue and the return of the writs. In particular this will include observing the set of test votes being passed through the system once nominations have closed and shortly before voting commences using the iVote® system, plus observing the ‘decryption ceremony’ at the close of the election, when electronic votes within the iVote® system are decrypted to be counted and are also checked against the voter-verified votes within the verification server.

Voter Distribution Check

This check will utilise the profiling of the traditional voting channel results versus the iVote® system results to assess anomalies and comparable distribution. Since electronic voting will comprise no more than 15% of the votes cast for any one electoral contest, it will allow comparisons of results with other voting channels which should have similar electoral demographics. Hence a substantial difference in the percentage of first preference results by candidate or group could highlight if tampering has occurred within the electronic voting channel.

Vote Count Check

All iVote® preferences will be published and be available to download and count. Therefore anyone can check that the final results of the election count are the same as the count they have done using the published preferences.

10.2.3 Independent Auditors

Auditors will review the performance, security and integrity of the iVote® system for the SGE 2015 . The audit reports will be made public in order to provide assurance in the overall process and use of iVote®.

iVote® Registration Check

NSWEC will record and report the number of electors requiring re-registration, declaring they did not register when sent a letter advising of a registration in their name, or advising of problems accessing the electronic voting system. All such incidents will be reviewed by an independent auditor to ensure the integrity of the iVote® system.

Assurance Vote Check

Independent auditors will confirm that the electors' votes as cast are in aggregate the same as the votes decrypted at the close of the election. This will be achieved by observing the Audit Verification process where both NSWEC and independent people will compare the decrypted votes from the core voting system that will be counted, with the votes in the verification server that have been verified by voters.

Audit Reviews

An independent auditor will review the implementation and operation of the system and provide an audit report to the NSWEC for public disclosure. The audit objective is to review the iVote® Remote Electronic Voting System in accordance with the Parliamentary Electorates and Elections Act 1912, No 41, Part 5, Division 12A, 120AD: Independent Auditing of Technology Assisted Voting. Audits will be provided to the Electoral Commissioner:

- at least 7 days before voting commences in each Assembly general election at which technology assisted voting is to be available, and
- within 60 days after the return of the writs for each Assembly general election at which technology assisted voting was available.

Without limiting the content of the audit, the independent auditor will determine whether test votes cast in accordance with the approved procedures were accurately reflected in the corresponding test ballot papers produced under those procedures.

The audit reviews will include the reviewing reports and documentation from the following security related activities:

- Security testing (penetration testing, application code testing and cryptographic testing)
- Infrastructure security including monitoring and alerting processes
- NSWEC Security test summary.

10.2.4 iVote® Users

The voters using the iVote® system will have a number of direct security controls at their disposal to ensure their vote is cast and counted as intended.

Vote-as-Cast Verification

At any time prior to close of voting, electors will be able to verify that the system has captured their vote as submitted.

To protect against an attack on a voter's PC or other internet connected device via virus or other malware, the Verification Service is only available via telephone to ensure verification cannot be impacted by infections of a voter's PC.

Vote-as-cast verification will be via an automated IVR telephone system. Access to the Verification Service will require the credentials (iVote® Number and PIN), plus the receipt number to be entered via the telephone keypad. The system will read out to the voter the ballot preferences for each ballot in order, with options for the voter to replay as needed to ensure all preferences can be clearly checked.

This will allow voters to verify their vote has been received and stored exactly as cast. The system will provide options for voters to be transferred to the call centre if they believe that the vote read back to them differs from what they cast. The system will record the number of votes that have been verified, including how many voters indicated the vote was not as they remembered casting it.

The iVote® call centre operators will allow the voter to re-register (thereby removing the original vote) and cast another vote if they believe the Verification Service did not read the vote back to them as they recall casting it. This provides an option for coerced electors to cancel the coerced vote and cast a new vote to their own intentions. This option also eliminates vote buying because a buyer could not be certain that the vote seller will not subsequently re-register and cast another vote to their own intentions.

It is likely that most voters calling to re-register 'because their vote did not match when verifying', will be doing so because they have either forgotten how they voted or simply want to change their vote. However, it is possible that vote verification was different from the vote cast, because malware on their PC had successfully changed the vote before being encrypted and sent to the iVote® servers. All instances of electors claiming that the verification showed their vote was different from cast will be logged and investigated, and through call-centre FAQ documentation, electors will be informed about virus and malware prevention and detection, and be advised to switch to a different, more secure device when voting again.

Vote counted Verification

After close of the election, electors will be able to confirm that their vote was counted by entering the Receipt Number provided to them at the time of voting, on the receipt checking page on iVote® website. The receipt number provided by the voter will be confirmed to the elector as having been included in the count.

If the receipt number does not represent a vote that has been counted, the voter will be provided the reason it was not counted, typically because another vote had been accepted via a different voting channel, such as postal or pre-poll.

Registration Impersonation Check

As part of the iVote® registration process, electors are invited to provide a driver's licence or passport number, as assurance against impersonation. In the absence of one of these, an acknowledgement letter is sent to the enrolled street address (or the enrolled postal address if one exists) of the registering iVote® user. Electors will be invited to contact the call centre if they had not registered.

This approach will identify potential impersonation and allow the NSWEC to cancel the impersonated vote prior to the close of the election. In addition, any evidence of such a fraud will be investigated and handed to the appropriate authorities.

A legitimate, eligible voter can re-register for iVote®, if they want to use the system, or cast their vote via another channel of voting.

Voter Coercion - Re-Register & Re-Cast Vote

If a voter feels they have been coerced into voting against their intentions they will have the ability to re-vote and also report such security incidents, which will be investigated.

Voters will have the option to re-register and re-vote by contacting the registration call centre. Provided the NSWEC call centre operator is able to confirm the voter's identity, the voter will be issued a new iVote® number. This process cancels the current vote and allows a new one to be cast by computer or phone as previously.

Call Centres

Call centres will provide support to electors helping them with registering and voting and any verification. These staff will provide the direct human interface of the iVote® system and through appropriate questions and analysis determine if the iVote® users has a legitimate security concern that can then be raised for further investigation. Importantly, the call centre can not only assist iVote® users in processes such as re-registration, but also provide assurance as the people element of the system.

Post iVote® Survey

After the iVote® period NSWEC will conduct a survey of electronic voters. The survey will, amongst other issues, assess the trust and perception of security in the iVote® system.

10.2.5 Physical Access

Decryption/Counting Room Access

The decryption ceremony at the close of the election will be attended by many people, with clear separation between participants in the process and observers.

Only approved NSWEC staff and independent participants will be allowed in the area where the votes will be decrypted and where the independent participants will verify the count and decrypted votes to the voter-verified votes from the independent Verification Service. Election observers, including scrutineers from Registered Political Parties will be admitted into the non-restricted area of the room to view the decryption, counting and verification processes, which will be presented on large screens. Explanation and commentary will be provided to assist the non-technical audience in understanding the process they are observing. This control allows transparency of the system to the public and political parties, providing assurance of the final count and trust in the use of the iVote® system.

Physical Access Control - Registration system

The registration server is located in NSWEC server room and access to the room requires approval from the NSWEC CIO. NSWEC Staff and Contractors gain access using their proximity card and the room has camera surveillance.

Physical Access Control - Core Voting System (CVS)

The CVS will be hosted in the NSW Government Data Centre, a tier 3 data centre. Cameras and security guards are used to ensure that only approved personnel enter the building. When personnel enter the building they are required to check-in by signing in with security to ensure they are permitted and understand the conditions for the data centre. Staff are required to be pre-approved before going to the data centre which ensures that even though they work for the company they have a purpose for being there. Access control at the facility includes “man traps” where a person passing through a first layer of security, such as through use of a stolen access card, would be trapped by the second layer, such as an iris scanner, and require security staff to release them. Data centres are unmarked buildings so the general public are unaware of what is contained inside.

Physical Access Control – Verification system

The verification system will be located in an independent data centre provided by AC3 (Australian Centre for Advanced Computing and Communications) who will operate this service independently from NSWEC during the election period. The auditor will also monitor the provision of this service. Physical access control will be commensurate to a tier 3 data centre.

General Office

NSWEC’s office operates with appropriate access and security controls. The staff/contractor security awareness training will provide further defence against social engineering attacks.

10.2.6 Testing

There will be comprehensive system and process testing conducted to ensure the system operates as per specification and security processes are in place and effective. This will be done before and during the election event.

Immediately prior to the election, testing of the system under simulated voting conditions and scenarios will take place to test for security event monitoring and that corrections occur within an acceptable timeframe.

During the election no specific security process testing will take place. However to test the system in its entirety, a dummy voter will be present in the registration system and not known to the core voting system, and can cast a vote which will be indistinguishable from any other vote cast. Dummy votes are encoded and decoded just like any other vote. The dummy votes are able to be identified through a unique preference pattern and can be retrieved from the election output prior to the commencement of counting. The only feature that a dummy vote will have to distinguish it from any other vote is the unique preference arrangement. If more than one live vote has the preference arrangement, then only the number of votes corresponding to the number of dummy votes cast for the election contest will be identified and removed.

10.2.7 Security Incident Management

A comprehensive security incident management strategy will be put in place to provide a cohesive security function across all of the various systems and key stakeholder groups. The strategy will provide for effective security management of an incident, from monitoring, identification and action to resolution.

NSWEC will use a Security Incident Response Plan to help deal with any incident in a way that limits damage and reduces recovery time and costs. The Security Incident Response Plan will include a definition of an incident and how to rate its level of severity. If an incident occurs it will provide a step-by-step process, based on the severity, which will be followed. This plan will also outline who will be involved in the incident management process, in addition to the iVote® team and IT Staff; representatives from legal, human resources or public relations departments may be included. Once resolved, a post incident review will be conducted to identify root cause and lessons learnt to proactively prevent the incident from reoccurring.

10.2.8 Change Management

Change management will be used by NSWEC in order to manage the risk of unauthorised changes and the impact of failed approved changes to the iVote® system.

Pre iVote®

Security will be an integral part of change management to ensure no further security risk are introduced into the environment during the design, testing and improvement phases of iVote®.

During iVote®

Once the iVote® system is live, changes to the infrastructure will be circumvented due to the lockdown. In the circumstance where a critical change would be required (e.g. in response to an incident), it would still go through NSWEC's change management process and would require approval from both the Commissioner and CIO. There will be no maintenance windows for software updates to the Core Voting System during the iVote® operational period, which includes the voting period and counting.

10.2.9 Release Management

Release management applies during the planning, design, build, configuration and testing of hardware and software for iVote®. Once the final, tested versions of software and infrastructure are approved they will be locked-down, preventing changes. The production release of CVS software will be digitally signed so that it can be validated at any time during the election that the software running the election is the correct, unaltered release.

10.2.10 Configuration management

As part of the iVote® quality system there is a Configuration Management Plan that defines procedures for:

- Identifying all the configurable items involved in the voting system;
- Change control, which requires that all changes to the configurable items are identified, properly authorised and incorporated throughout their lifecycle; and
- Auditing the status of configurable items to ensure their accuracy, correctness, completion, and integrity.

10.2.11 Capacity Management

Capacity management ensures that the iVote® system and infrastructure has the capacity to deliver the services to meet voter demands. This will include the capability to manage DDoS attacks that would directly affect the ability of the iVote® system to meet voter demands.

Capacity analysis and planning have been integral to the iVote® project from the beginning and the usage models and analysis are frequently re-assessed with the review of assumptions made in usage estimates. The system will undergo extensive performance testing, including load testing to confirm that required loads are supported without any performance degradation, and also stress testing, where the system is tested to capacities well beyond the required load and also beyond the design load, to the point of failure. The stress testing allows maximum capacity limits to be measured and confirmation that exceeding this limit does not cause catastrophic failure, but a graceful degradation of service.

10.2.12 Availability Management

NSWEC aim to have no interruptions to the iVote® service, with full 24/7 availability during the voting period, however iVote® will have alerts and alarms to report system outages. iVote® will be designed to achieve a minimum 99.9% uptime with 15 minutes recovery time objective in case of outage.

Note that these uptime and recovery-time goals are lower than that of most banking and e-commerce sites, which adopt complex high-availability infrastructure to achieve minimal disruptions to services that run 24/7 for year after year. The NSWEC approach is based on an appropriate balance between the risk of hardware failure and complexity, where the risk of hardware failure within the 13 day voting window is very low due to the shorter timeframe and the added complexity would bring additional security and infrastructure failure risks.

10.3 Technology

Technical security controls are used to reduce the exposure of the iVote® system and protect the data. Technical controls include all software and hardware used to operate the iVote® system.

10.3.1 iVote® Application Components

iVote® comprises multiple components that form three primary groups:

- Registration System
- Core Voting System (CVS)
- Verification Service

Each group of components are hosted and managed separately.

10.3.1.1 Registration System

The registration system provides an inherent security feature of recording a six digit PIN that is only known to the elector and can then be used as one of the credentials necessary to access the iVote® system to lodge their vote in the election period. Once enrolment details are supplied and eligibility is confirmed, a PIN is received from the elector by the Registration System. The NSWEC then provides the elector with a unique electronic vote identifier (the iVote® Number). Only when both the PIN and iVote® Number have been distributed can the electronic vote be created and made available for the elector to vote.

Security of the iVote® PIN

The NSWEC will not hold the elector's PIN as it is immediately hashed and encrypted by the Registration System and passed to the Credential Management system for storage. No copy of the PIN, either in plain text or the encrypted version, is retained by the registration system.

Credential Management System

The Credential Management System is a key part of the registration process and integral to security and vote privacy. It is responsible for managing the NSWEC's correspondence with electors about their iVote® registrations and for issuing and, if required, re-issuing the iVote® number that is used to access the Core Voting System.

The Registration system is an online system supporting electors and call centre operators with the iVote® registration process. Required within the registration system are the enrolment details of all NSW electors, so the Credential Management system maintains separation of this information from any data about an elector's use of iVote®.

The Credential Management System controls unique 'credential hashes' for each registration. The use of the 'credential hash' allows the iVote® number to be known only by the Credential Management System, with the CVS knowing only the credential hash, which is sufficient for it to validate the iVote® Number and PIN of a voter logging in to CVS to cast their vote.

After close of polls, Credential Management interfaces with EMA for elector mark-off and for determining and removing multi-votes.

One-use iVote® Number

The iVote® Number and the hashed PIN are used to create the hashed credential, which is retained by both CVS and Credential Management. Encoding of the combined credential to a hash will be done using a secret Salt to limit the possibility of brute force decryption by an external attacker. The separate Credential Management system prevents an attack on the CVS from being able to determine an elector's PIN and iVote® Number.

Once a valid credential has been used to submit a vote, the credential cannot be used again. If a voter chooses to re-vote the voter must re-register so that a new credential is created and the old one, together with any vote preferences attached, is removed. However, if a voter has not submitted their vote they are able to log on again using the same credential to recommence voting at the point where they left off.

Election Management Application (EMA) interface

The interface between Credential Management and EMA provides a facility to update EMA regarding those electors who have registered for iVote® , and for voters who already have an accepted vote through another voting channel recorded in EMA, to be identified and their iVote® to be removed before it is decrypted for the count. EMA also records the acceptance of an iVote® for all voters who have successfully completed an iVote® that is to be counted, which then prevents a postal vote being accepted for those voters at a later time.

10.3.1.2 Core Voting System

Ballot Controller

The Ballot Controller module is responsible for generating a unique credential hash. It derives the Credential Hash by using the hash of the voter generated PIN number and the iVote® number sent from the Credential Management, which is then mixed with a secret Salt. The Ballot Controller module confirms that the credential hash generated can uniquely identify a 'virtual ballot paper' before the credential hash is passed back with confirmation to the Credential Management System.

The Ballot Controller also validates the iVote® Number and PIN entered by the voter when logging in to the iVote® system to cast their vote. It does this by re-creating the hash of the PIN and then creating the credential hash to match against its store of valid credentials. Note that this connection between the vote and Credential Hash is deleted by the Vote Mixer, as part of the process of opening the ballot box.

Vote Encoder

The Vote Encoder is responsible for encrypting the vote preferences as submitted by the voter, to maintain the secrecy of the vote. The Vote Encoder encrypts the vote twice, with different keys, and after using a Zero Knowledge Proof to validate the two encrypted votes are the same, it sends one copy directly to the Verification Service.

The vote encoder sends a message back to the voter that their vote was successful and provides a 12 digit Receipt Number. It will also provide appropriate messages to the voter if the vote was not successfully received and processed.

Vote Mixer Module

This component is responsible for separating the encrypted vote from the Credential Hash to remove the link between the voter and the cast vote. This function is equivalent to the act of the voter putting their completed ballot papers into the ballot box at the voting venue. This addresses the security principle of the secrecy of the vote. After separating the vote from the credential hash, it performs a mixing process to ensure that the separated votes are in a random order compared to either the order in which the votes were cast or any other sequence that could be used to identify the voter to which the vote relates.

Vote Decoder Module

This module is an offline component that only interfaces to other iVote® components through the transfer of files on portable media such as SD cards or USB memory sticks. It decrypts the votes once the virtual ballot box is opened and the votes are stripped of their credential hash and mixed. The Vote Decoder will generate the vote preferences in the clear for the count, together with its receipt number, which is then loaded to the receipt checking service.

The output of decrypted votes from the Vote Decoder supplies the audit process where the decrypted votes are re-encrypted to be compared and matched with those from the Verification Server.

Once the auditor confirms all votes match those kept on the Verification Server, the votes in the clear will be passed to the counting systems, including EMA and PRCC.

The Vote Decoder will also provide all receipt numbers of those votes that have already been audited and matched to those kept on the Verification Server. These are loaded to the Receipt Number website, which will provide facilities for elector to check their receipts.

Receipt Number Module

It allows the elector to confirm that their vote has been processed through the system and forms part of the count. The 12 digit numeric receipt number is created by the Core Voting System (CVS) at the time the vote is cast, but it is not stored in the clear during the election.

The receipt number website receives a list of receipt numbers of all iVote® s that were admitted to the count from the Vote Decoder. It is available after close of polls and after all data is received from the Vote Decoder, and is accessible by the Voter from the Monday after election day via the receipt number web site link provided by the NSWEC.

This provides assurance of the system overall and to the individual voter that their vote was counted as cast.

Voting Management Module

It supports the setup, configuration and administration of the iVote® CVS and of each election event. This includes the configuration of security components such as the election keys and admin board keys, digital certificates for security of interfaces, blocking access to remote voters at the close of the poll and the export of receipt numbers from the Vote Decoder to the receipt number system.

The Voting Management Module will provide assurance that the system and its key voting security components are in place and working as intended.

Ballot Box security

- Storage - the integrity and authenticity of the electronic ballot boxes will be protected by means of secure encryption of votes, digital signatures, combined with secure immutable logs.
- Ballot Controller - the Ballot Controller is the only module responsible for generating the unique Credential Hash (see above) required to cast a vote and controls all removals of votes if the elector has voted via another channel or if the elector re-registers for iVote®. Since the verification service receives removals directly from the Credential Management System, it is not possible to use the Ballot Controller to remove votes without being detected.

Virtual Ballot Paper (VBP)

The VBP is a concept within CVS representing the encrypted vote cast by an elector, which is digitally signed to protect against the vote being changed after it is sent from the browser. The signing is done within the voter's browser using PKI and a pre-generated private key at time of voting. The voter's certificate containing the public key is then used by the server to check the vote preferences were not changed.

10.3.1.3 Verification Service

The Verification Service allows a voter to confirm by telephone, using an automated IVR system, that their preferences were captured by the iVote® System correctly. At any time after voting and before the close of voting, the voter can call the service and enter their credentials (iVote® Number and PIN) using the phone keypad (DTMF) and then entering the receipt number provided to them upon submitting their vote. The system will use these credentials to decode the encrypted vote and read the preferences back to the voter.

This facility closes as soon as voting ends, to allow the connection between the encoded vote and the Credential Hash to be destroyed, thus reducing the risk of a breach to vote secrecy.

After close of polls, but before decoding votes with the election key in the Core Voting System, the Credential Hash is also removed from the encrypted votes held on the Verification Server and these are then provided to the audit process.

Audit process

The Audit process allows the votes passed through the Core Voting System to be compared to the votes as captured at the time of voting and placed on the Verification Server. This comparison is done without revealing the voter preferences or the voter's identity.

The audit process will occur with observers present and will involve independent people simultaneously performing the same process as NSWEC will perform to compare the votes going into the count with those from the Verification Service.

NSWEC will have software to:

a) count the decrypted votes, and

b) re-encrypt the decrypted votes and match to the Verification Service votes.

While NSWEC will make this software available, it will also provide sufficient technical details to the independent people for them to create their own software to confirm that the votes deliver the same count and are a match between the CVS and the Verification Service.

The auditor will be an observer of this process and declares the votes to be counted have not been tampered with when all parties have been able to confirm that votes emitted from the CVS ballot box for the count match the votes held on the Verification Service.

10.3.2 Security Monitoring

System Logging

All components of the iVote® system will provide substantial logging of events, activities and any errors that occur, including infrastructure and configuration changes. The logs will be immutable and stored both locally and sent to a central repository. The logs will not capture information which could allow the preferences in a vote to be explicitly associated with a given voter.

A dashboard facility will provide continuous display and monitoring across all log events, with alerts configured for all critical events. This dashboard will also provide regular reports on usage across the system in terms of registrations, voters, completion rates, time taken to vote etc.

Security Operations Centre (SOC)

A tier 1 third party provider will be used to provide SOC functions that will include a Security Information Event Management (SIEM) solution to collect all security event logs, correlate monitoring and provide analysis on a 24x7 basis. The SOC will be staffed by specialist security analysts, integrate threat intelligence feeds and have higher level tiered security engineers to provide focused security response to an incident. The SOC will be integrated into the NSWEC operations for the SGE 2015 with their processes and procedures.

10.3.3 Application Security

Application Authentication

The voting system will have access control mechanisms designed to control voter access to the voting system web site based on the mode and venue associated with the voter’s access device.

The voting system will authenticate per the minimum authentication methods outlined below.

GROUP OR ROLE	Identifier	MINIMUM AUTHENTICATION STRENGTH
Voter	iVote® Number	iVote® Number and PIN
NSWEC	Application or operating system account	Two-factor (after lockdown, only application access allowed)
Application or Process	Operating System account	Digital Certificates associated with all interfaces, plus lockdown of traffic to specific IP addresses.

Application Logging

The logging module will provide high-level status of the election process clearly showing the processing of votes through the system. It will monitor the relationship between votes cast and registered voters and show when the aggregate voting position is outside expected tolerance. It will also allow deep-diving into detailed transactions without revealing how a given elector voted.

Secure Code Review

An assessment of the source code will be conducted against internal/industry security coding standards. This will be performed by experts selected by NSWEC for their expertise in electronic voting systems. The critical software elements of the iVote® system will be independently reviewed by these experts at the code level, to identify any potential flaws or issues that might allow security breaches or could reduce public trust in the votes collected by the software.

Web Application Firewall (WAF)

A Web Application Firewall will be deployed behind the network firewalls, in front of web applications. This will provide protection against Denial of Service layer 7 attacks, block known and unknown attacks against web and web services applications, filter communications at the application layer, scan and protect known application vulnerability. In addition it will analyse all bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats without any modification to applications. Security event logs from the WAF solution will be sent to the SOC for real time monitoring

10.3.4 Infrastructure Security

Infrastructure will be designed and built to enable the iVote® system to provide a secure and highly available production environment. The infrastructure will provide services to support the operation of the Core Voting System.

Anti-Malware software

All systems will have commercial grade anti-malware software installed in order to protection from malware and viruses that will be managed and monitored as a key defensive measure. Security event logs from the anti-malware solution will be sent to the SOC for real time monitoring

Vulnerability scanning

Will be used to detect, identify and report on any security weaknesses in the environment. This will assist with the assessing the security configuration of the environment against stated policies as well as allowing for any additional measure to be taken to address new flaws. Security event logs from the vulnerability scanning solution will be sent to the SOC for real time monitoring.

Patching

Operating system patching will be performed in line with the election lifecycle and NSWEC policies. Patching will be limited to assessed critical patches during the iVote® system lockdown to maintain the balance of assurance of the system being un-tampered and the threat that any patching may bring to the system if left unattended.

Operating System Standards

All server operating environments will be deployed following Standard Operating Environment guidelines and checklists which will be developed to ensure appropriate hardening is provide for the application function supported

10.3.5 Encryption

Envelope Generation

The voting client generates two envelopes encrypting the voting options: one under the Electoral Board's public key (envelope for counting), and another one under the Verification Service public key (envelope for verification). Other data generated at the voting client and included in the envelopes is a Receipt Number, which is a value that must be unique to that vote (and thus this is checked by the server-side), and a Random Extension (an extension to ensure encryption strength for the verification envelope, through sufficient key-length).

Proof Generation

The voting client also generates some Zero-Knowledge Proofs, to prove that: both envelopes contain the same voting options, the ciphertexts have been freshly generated and have not been copied from the vote cast by another voter (plaintext independence), and that the Receipt Number inside the envelopes matches the one provided to the Vote Encoder to check uniqueness.

Vote Casting

The two envelopes and the proofs are sent to the Vote Encoder, who verifies the proofs.

Vote Storage

The Vote Encoder forwards the second envelope to the Verification Service, and stores the first envelope in the Ballot Box database.

Ballot Box exporting

Once the voting phase ends, the first envelope and some of the proofs are exported from the Vote Encoder, to the Mixing module. Amongst other validations, the exported proofs are verified at a cleansing step within the Mixing module.

Votes Decryption

Once the envelopes are shuffled and decrypted to obtain the cleartext voting preferences and Receipt Numbers, a Zero-Knowledge Proof of correct decryption is generated to prove the correctness of this process.

10.3.6 Security Trust Model

A Security Trust Model is a zoned network providing defence in depth for sensitive information resources and deployment of platforms and controls in accordance with security principles, policies and standards.

A given system or network is considered to be suitable for a particular security zone if it meets a set of predefined criteria or characteristics. There will be instances where a system does not meet the criteria. In these instances, additional controls will need to be implemented and where applicable, greater levels of assurance of existing controls (and their effectiveness) need to be obtained.

The layout of iVote® networks will provide for the separation of systems by purpose and access requirements based on the predefined security and trust zone models. All traffic traverses between the zones is screened through the use of firewalls, secure VPNs (Virtual Private Networks, including the NSW Government Private Network) and Access Control Lists (ACLs). The separation of systems reduces the potential impacts of a security breach by restricting the effects of additional attacks and isolating individual system domains.

NSWEC Office LAN clients are not given unrestricted access to the iVote® systems and all traffic is screened through the use of firewalls and Access Control Lists (ACLs).

10.3.7 Data Centres

The iVote® Core Voting System and Verification Service will both be hosted in at least tier 3 data centres, separated from the NSWEC's own network, registration system and from each other. These systems will also be managed independently with clear legally enforceable reporting responsibilities for each system's manager. This approach will reduce the risk that a single breach of security of any one system or management group would impact voter secrecy or vote integrity.

10.3.8 Network Monitoring

All network monitoring controls will be further monitored, aggregated and analysed by the Security Operations Centre. The following are specific controls that will be used:

Independent secure NTP

The clocks of all servers are synchronised using an independent NTP source to avoid any tampering that could lead to exploitation of the logging systems and security monitoring.

Intrusion Prevention Systems

Intrusion Prevention Systems (IPS) will be deployed on the public facing network segment and the segments containing business critical and sensitive applications and data. The IPS to be implemented is expected to incorporate network-based, host-based, and application-based sensors based on the criticality of the information being protected. Security event logs from IPS will be sent to the SOC for real time monitoring.

Routing

All internal network routing between computers and network devices will be configured in such a manner as to ensure, during normal operation, data can only travel to those computers and ports required to operate the iVote® system. This will reduce the attack surface available to a threat and provide connection assurance.

Firewalls

Every entry point into iVote® networks will be protected by an appropriate, stateful firewall service. Two-tier firewall services will be deployed for the iVote® networks to achieve the required depth of security. Firewall clustering may be implemented at each site to improve the service availability. Security event logs from the firewalls will be sent to the SOC for real time monitoring.

DDoS protection

A third party provider will be used to mitigate DDoS by automatically detecting all types of attacks launched against the website and web applications, focusing on layer 3 and 4 protection, with the WAF providing the layer 7 OSI DDoS protection. They will also be used to safeguard the critical network infrastructure from protocol-based attacks.

DNS

The solution will monitor and assess all changes made to the DNS service to validate they have been appropriately authorised and block any malicious queries. Security event logs from the solution will be sent to the SOC for real time monitoring.

File Integrity Monitoring (FIM)

A FIM solution will, be used to defend against replacement or modification of executable or interpreted code as well as preventing access to or manipulation of configuration data, vote data, or audit records. FIM controls look for unauthorised changes to the system that could be the result of nefarious activity. Security event logs from FIM will be sent to the SOC for real time monitoring.

Threat Intelligence

A Threat intelligence feed will be provided by the SOC and used for correlation and analysis against the individual security event logs. Custom threat intelligence feeds will also be developed based on the strategic threat analysis

10.3.9 Distributed Security Assessment Review

A comprehensive security assessment of infrastructure, platform and application security components and dependencies will be conducted prior to the system going live. This will include the following:

Vulnerability and Penetration Testing

Hardware and software shall be penetration tested by qualified technicians prior to commencement of the voting period and shown to be resistant to known relevant threats.

System Image

Snapshots of the system will be taken by an auditor during the system's operational period at times selected by the auditor and then compared to a benchmark approved system.

Security Functional Testing

Analysis of system to ensure security devices and controls are working as intended, including generating the required logs for the technical controls.

10.3.10 Disaster Recovery

The three separately hosted iVote® systems will be continuously replicated to their respective DR sites. The NSWEC will ensure that the iVote® system is fully backed up periodically during operation to an independent site. This will allow audit verification of the system in various stages of the election should it be needed and allow recovery should both the primary and replicated system become corrupted or destroyed.

10.4 Other Controls

10.4.1 3rd Party Security Incident Response

A third party provider will be on standby to provide major security incident response and forensic capability in the event of a security incident. This will allow NSWEC to provide the additional expert resources at short notice should an incident occur and rapidly work towards a resolution.

10.4.2 Strategic Threat Actor Monitoring

Will provide advanced warning of any threat changes in motives, modus operandi, capability, intentions or affiliation. This is achieved through back-channel monitoring of threat groups through industry experts and government intelligence agency liaison.

10.4.3 New Controversial / Emotive Legislation

NSWEC will monitor any new (or proposed changes to) legislation or policy that could be seen as controversial to either the public or threat actors. Identification of any heightened tensions around new legislation or policy could warrant the focus of further monitoring efforts on associated groups that may target SGE 2015 and the iVote® System.

10.4.4 NSW police, AFP and Australian Intelligence Community Liaison

Will assist NSWEC with any known criminal groups, criminal elements or potential individual suspects that may have the capability and the desire to target iVote® for the SGE 2015.

10.4.5 Media Coverage

NSWEC will monitor the media for any events that might act as a catalyst or be a potential pre-curser to an attack. Areas of interest would include International affairs where Australia might become a target for controversial policy or actions, increased national or international general media coverage of the SGE 2015 and its use of electronic voting, or any actions or rhetoric by known threat actors that could result in attacks.

10.4.6 Community Awareness

The NSWEC will implement a public information and education campaign prior, during and post the iVote® system going live, to ensure electors are aware of the security and secrecy features of the iVote® system.

NSWEC will continue its ongoing consultation with low vision and disability bodies to ensure all critical aspects of their requirements are satisfied and the most appropriate solution for NSW is implemented.

Promotions

Promotions directed to particular target groups include:

- Blindness and disability support groups
- Direct to mail remote electors
- Radio advertising on 2RPH
- Call-out campaign by Vision Australia

Advertising and awareness campaigns prior to iVote® including:

- Print - Two weeks of print advertising across NSW
- Posters - iVote® posters in Returning Officer offices and other locations
- Internet advertising - targeting electors outside NSW
- Social media - Facebook, Twitter and YouTube promotions
- Industry awareness - Through presentations such as AusCert presentation – During the May 2014 AusCert conference the NSWEC CIO presented on iVote® and its use for SGE 2105.

Transparency

- Tally check - provide a full list of all formal votes with all preference markings for any member of the public to undertake their own vote count and compare to the results published on the NSWEC virtual tally room website.

- Source code review - Will be available for inspection to suitably qualified persons who are willing to comply with the NSWEC’s terms of engagement.
- System documentation available to the public - the NSWEC will publish review documents provided as a result of work completed with a NSWEC response. The NSWEC will also publish key project documents during the course of the project.
- System logs available to the public - The iVote® logs during the voting period will be available for inspection by suitably qualified persons who are willing to comply with the NSWEC’s terms of engagement, during and after the election to the extent legislation allows and to a level which will ensure the secrecy of an elector’s vote and system integrity. These logs will be used to ensure that the votes counted match the votes entered and the system has not been compromised.

11 Controls mapped to principles

The following table maps the security controls to the principle and also outlines where the controls are found in the documentation.

iVote® Control mapping				
iVote® control		Principles	NSWEC Documents (Policy, Standards, Procedures)	Attribute
No.	Description			
10.1	**People**			
10.1.1	Staff Management	Comprehensible, Assurance	HR documents	Prevention
10.1.2	Election Specific Employment	Comprehensible, Assurance	HR documents	Prevention
10.1.3	Clear Roles and Responsibilities	Comprehensible, Assurance	HR documents	Prevention
10.1.4	Separation of Duties	Comprehensible, Assurance	Operating Procedures	Prevention
10.1.5	iVote® Manager	Comprehensible, Assurance, Integrity, Availability	Approved Procedures	Prevention
10.1.6	Security Awareness and Training	Comprehensible, Assurance	HR documents plus iVote call centre training	Prevention
10.1.7	Monitoring of the Workplace	Assurance, Integrity	HR documents	Prevention
10.1.8	Stakeholder Groups	Assurance	Community consultation plan	Prevention
10.2	**Processes**			
10.2.1	System Access Control	Assurance, Integrity	Lockdown procedures	Prevention
10.2.2	Integrity Checks	Assurance, Integrity	Operating procedures	Evidence
10.2.3	Independent Auditors	Comprehensible, Assurance	Audit reports	Evidence
10.2.4	iVote® Users	Comprehensible, Assurance	Logs of verifications etc.	Evidence
10.2.5	Physical Access	Assurance, Integrity	NSWEC + data centre procedures	Prevention
10.2.6	Testing	Assurance, Integrity	iVote Test Strategy	Prevention
10.2.7	Security Incident Management	Assurance, Integrity and Availability	Security Incident Plan	Prevention

iVote® Control mapping				
iVote® control		Principles	NSWEC Documents (Policy, Standards, Procedures)	Attribute
No.	Description			
10.2.8	Change Management	Integrity and Availability	Change Control Procedures	Prevention
10.2.9	Release Management	Integrity and Availability	Scytl Release Management	Prevention
10.2.10	Configuration management	Integrity and Availability	Configuration Mgt. Plan	Prevention
10.2.11	Capacity Management	Assurance, Integrity and Availability	Test Strategy	Prevention
10.2.12	Availability Management	Assurance, Integrity and Availability	Data centre Procedures	Prevention
10.3	**Technology**			
10.3.1	iVote® Application Components	Assurance, Secrecy		Evidence & Prevention
10.3.1.1	Registration System	Assurance, Secrecy	Specifications documents	Prevention
10.3.1.4	Core Voting System	Assurance, Secrecy	Specifications documents	Prevention
10.3.1.7	Verification Service	Assurance, Secrecy	Specifications documents	Evidence
10.3.2	Security Monitoring	Assurance, Integrity and Availability	Security Operations Centre Procedures	Evidence
10.3.3	Application Security	Integrity, Availability	Source code review report	Evidence & Prevention
10.3.4	Infrastructure Security	Integrity, Availability	Infrastructure documentation	Prevention
10.3.5	Encryption	Integrity	Source code review report	Prevention
10.3.6	Security Trust Model	Assurance, Integrity, Availability	Lockdown documentation	Prevention
10.3.7	Data Centres	Assurance, Availability	Secure Logic and AC3 procs	Prevention
10.3.8	Network Monitoring	Integrity, Availability	Security Operations Centre (SOC) Procedures	Evidence & Prevention
10.3.9	Distributed Security Assessment Review	Assurance, Integrity, Availability	CSC threat assessment report Penetration testing report	Prevention
10.3.10	Disaster Recovery	Assurance, Integrity, Availability	Failover procedures and failover test results	Prevention

iVote® Control mapping				
iVote® control		Principles	NSWEC Documents (Policy, Standards, Procedures)	Attribute
No.	Description			
10.4	**Other Controls**			
10.4.1	3rd Party Security Incident Response	Assurance, Integrity, Availability	CSC SOC escalation procedure to worldwide security team	Prevention & Evidence
10.4.2	Strategic Threat Actor Monitoring	Assurance, Integrity, Availability	CSC custom SOC monitoring	Prevention
10.4.3	New Controversial / Emotive Legislation	Assurance	NSWEC liaison with Premier's Department	Prevention
10.4.4	NSW police, AFP and Australian Intelligence Community Liaison	Assurance, Integrity, Availability	NSWEC liaison with NSW Police and CSC liaison with AFP and intelligence community	Prevention & Evidence
10.4.5	Media Coverage	Assurance	NSWEC media monitoring	Prevention
10.4.6	Community Awareness	Assurance	iVote Marketing Strategy	Prevention

12 Documentation

Documentation forms an important part of the processes for the use of IVote® in the SGE 2015. The following existing and planned documents provide details of the operation of iVote®, the interaction between the other voting systems and the people component of the system.

12.1 iVote® overview document

An iVote® technical system document based on an original version created for the Request For Tender (RFT) for the CVS, its purpose is to provide an overview of iVote® in its entirety and covers all 3 primary systems including security aspects

12.2 Risk Register

- NSWEC Risk register 2015 SGE

12.3 Policy (Must be met)

- NSWEC Information Security Policy (existing, as noted in iVote document A7)
- iVote® Security Policy
- Council of Europe Recommendations – Appendix B

12.4 Standards (Guidelines of how to meet the policies)

- NSWEC Information Security Standard (includes all security controls – including zoning)
- Logging standard (platform and application – iVote document A6 – 5.8)
- iVote® hardware and software standard
- Security and function test plan
- Privacy standard
- Configuration standard (iVote document A6 -7)

12.5 Processes and procedures (including RACI)

- NSWEC SGE 2015 process and procedures
    - Registration system procedure
- iVote® practices and procedures overview
    - System Operation Manual (iVote document A6 - 8.6)

    - Configuration control procedure (iVote document A6 -7)
    - Software hardening procedures (iVote document A6 – 8.4.1)
    - Functional and Security system testing procedure
    - System Administrator procedure document – pre and post lockdown – access, dual authorised access, restricted once live, remote access (iVote document A6 – 8, 8.3.1, 9.3.2)
    - Physical access procedure – datacentre, auditor, offices, 3rd party providers
    - Call centre procedures – How to support / use iVote® , Incident resolution
    - Counting system procedure (EMA & PRCC procedures)
    - Verification server procedure (Verification Service document A1 – V-2-2A, V-2-2B)
    - iVote® cryptography procedure (iVote document A6 – 5.6)
    - Database procedure
  - Registration system
    - iVote® registration system procedure (include information from iVote document A1 – R-1-5, R-1-5, R-3-5, R-4-5,R-5-5 need to add RACI)
    - iVote® self-service registration system procedure
    - iVote® number generator system procedure
  - Credential management system
    - Credential management system procedure
  - Core Voting System procedure (iVote document A1 - V-1-2)
    - Voice Server procedures (iVote document A2 - 2.6)
    - Web server procedures (iVote document A2 - 2.7)
    - Ballot Controller procedure (iVote document A2 - 2.8)
    - iVote® Encryption procedure (expanded from iVote® encrypt process with verify and audit) (iVote document A2 – 5 – Hashing and encryption process)
    - Vote Encoder procedures (iVote document A2 - 2.9)
    - Vote Mixer procedure (iVote document A2 - 2.10)
    - Vote Decoder procedure (iVote document A2 - 2.11)

        - Voting Management module procedure (iVote document A2 - 2.12)
        - Receipt number website procedures (iVote document A2 - 2.13)
    - Vote auditing procedure (iVote document A1 – A-1-1)
        - Voting integrity check procedure (comparison of traditional vote profile to iVote®)
    - Voting
        - Remote venue procedure (iVote document A1- 4.3 process only)
        - Attendance voting procedure (iVote document A1 – 4.4)
- Security Operations procedure – education, handover, access, monitoring, management - escalation process/contacts including management of security controls (3rd party, NSWEC and SOC provider)
- Security Incident response procedure Disaster Recovery Procedure

13 Conclusion

The NSWEC iVote® Security Implementation Statement provides an overall view of the security that will be in place for the SGE 2015, along with linkage to the further detailed documents. The statement outlines the integrated security strategy with the focus of a complete security system that encompasses people, process and technology. NSWEC understands that a system cannot be 100% secure, and has focused the strategy on a risk management approach to have a high level of security, but importantly controls in place that will allow for the detection of a security incident that may affect the outcome of the voting results from iVote®.

The key people controls are around the responsibilities of the NSWEC staff, system administrators, third parties and voters. Having multiple trusted organisations providing different components of the service allows for a separation of duties and greatly reduces any collusion to affect a system. This is further reinforced with limited access and only key NSWEC staff having access to more than one system.

Security processes have been created to provide the linkage between the systems, the staff (people) and the technologies of the overall voting system. The processes require clear separation of duties for security functions and additional check processes are in place to validate the overall result. Processes are importantly also in place for the NSWEC Call centre and auditors who will have direct contact with the voter if there is an issue raised, that will be integrated into the security incident management plan. Lastly, processes will be created for the voter to make them aware of the correct procedure on how to vote and to raise any security issues with NSWEC or the auditor to allow for an investigation.

The security technology for iVote® has been architected in a defence in depth manner to protect the system. The iVote® application itself has a number of security functions that include logging, encryption, restricted configuration, locked down function and separation of functions that will translate to physical separation of systems. Additional security controls will also be layered that include traditional controls like firewalls, IPS, security information event management, file integrity monitoring, etc. Such controls provide both a preventative and evidence based system to thwart or recover from an incident. Also as part of the technology controls security testing of the system from code reviews, vulnerability, penetration and functional testing will provide assurance the system is working as intended from a security point of view.

These controls will address the core security principles and provide an eVoting system that has risks commensurate with that of the traditional voting channels. NSWEC will provide education and awareness campaigns (both official and unofficial) to promote the security of iVote® and its use in the SGE 2015.

Appendix A – Glossary

Term	Explanation
iVote® system	The NSWEC electronic voting system comprising software components, hardware, networking, procedures and protocols required to deliver remote electronic voting services for the benefit of eligible NSW electors.
iVote® Core Voting System (or Core Voting System)	The software components or modules subject of this RFT, as described in the iVote® high level solution architecture, together with their associated interfaces.
iVote® Core Voting System solution	The iVote® Core Voting System together with associated services for its implementation and support
Absent Vote	A vote made at a designated voting centre by an elector who is outside his or her own electoral district.
ASD	Australian Signals Directorate
Attendance Vote	A vote made by an elector in attendance at a voting centre within NSW (e.g. Sydney Town Hall - STH) where a NSWEC appointed official is available to supervise voting. *(Note: Current legislation only allows iVote® to be used at centres outside NSW, see "Remote Electronic Voting").*
By-election	An election held to fill a casual vacancy on a council or in the Legislative Assembly if an elected representative dies or retires.
Completed Virtual Ballot Paper (CVBP)	A used Virtual Ballot Paper containing the preferences as submitted by a voter on completion of the eVoting process.
Credential Hash	The Credential Hash is a number generated by combining the iVote® Number and PIN using a hashing formula. The Credential Hash will never be directly stored in the system, but an HMAC of it. The key used for the HMAC is such a size that it is extremely unlikely that some randomly selected input text could produce the same hash value. The hash is used to ensure the iVote® Number and PIN entered by a voter is valid by using the same hashing formula (see below) to convert the entered data which is then compared to the stored hash.
Credentials	Information used to identify an individual accessing the system – in the iVote® system for an elector this includes a PIN number known only to the elector and an iVote® number generated by the system.
Declaration Vote	A vote cast by an elector where the elector declares he/she is entitled to the vote. Typically the voted ballot papers are enclosed in an envelope containing a printed declaration signed by the elector. Envelope based declaration votes are postal votes, absent votes, enrolment votes and section votes. In district pre-poll and Declared Institution votes are cast as ordinary votes.

Declared Institution	A hospital, nursing home or other facility appointed by the Electoral Commissioner and visited by election officials to take votes from residents who are unable to attend a polling place on election day.
Disabled Voting	Voting by an elector who has a disability (within the meaning of the *Anti-Discrimination Act 1977*) and because of that disability has difficulty voting at a polling place.
District	Used for state elections, districts are geographical regions with clearly defined boundaries shown on electoral district maps containing approximately equal numbers of voters. Each district is represented by one of the 93 NSW Legislative Assembly seats. For the Legislative Council, the district is the whole state.
Election Management Application (EMA)	A NSWEC developed computer system to undertake administrative tasks including nominations; processing declaration votes and election results.
Elector	A person who is on the electoral roll and certified to vote in an election.
Hashed PIN	The result of applying a one-way cryptographic hash function to a PIN, supplied by an elector/voter. Only the hashed PIN is transferred between iVote® systems. The hash of the PIN is always stored encrypted.
Informal vote	A ballot paper left blank and that is therefore excluded from the count. It does not contribute to the election of a candidate.
iVote® system	The NSWEC electronic voting system comprising software components, hardware, networking, procedures and protocols required to deliver remote electronic voting services for the benefit of eligible NSW electors.
Legislative Assembly (LA)	The Lower House of the NSW Parliament has 93 Members, 1elected from each district.
Legislative Council (LC)	The Upper House of the NSW Parliament has 42 Members elected for an 8 year term, half of whom are elected at each general election.
Local Government Area	A subdivision of the state into geographical areas that councils are responsible for.
Nomination(s)	The process by which a person applies to become a candidate for a State or Local Government election. In this RFT used as a term for all data that is a result of that process.
NSWEC	New South Wales Electoral Commission (ABN 94 828 824 124)
Optional preferential (voting)	A voting system in which an elector shows by numbers their preferences for individual or groups of candidates but need not show a preference for every candidate or group listed.
PKI	Public-Key Infrastructure
PRCC	Proportional Representation Computer Count system
Referendum	A vote taken to allow electors to express their view on a specific subject or issue.

Term	Explanation
Remote Electronic Voting (REV)	Electronic Voting - From a location of the elector's choice using a device not provided or directly managed by the electoral authority. - At a voting centre that is located outside of NSW using a device provided by that voting centre (Remote Venue voting). Registration and voting are performed on same computer. - By phoning the Voting Call Centre. The call operators use the remote voting system on the elector's behalf and cast the vote under their instructions.
Remote Mobile Voting	Mobile pre-poll voting at remote locations across the State.
Pre-Poll (vote)	Electors who cannot vote on election day can vote early at a (pre-poll) voting centre; electors have the option of using iVote® , either Remotely (if eligible) or by Attendance in venues such as STH, to cast a pre-poll vote.
Secret Key for HMAC of Credential Hashes	Secret key that is used for creating the HMAC of the Credential Hash which is computed from the iVote® Number and hashed PIN
SGE 2015	The NSW State General Election to be held in March 2015.
SPID	SmartRoll Person ID. A unique voter electoral identifier (held in the electoral roll).
STH	Sydney Town Hall. A Voting Centre based in the Sydney Central Business District.
TPC	Two Candidates Preferred count. Two candidates preferred count refers to a distribution of preferences of the two candidates who are expected to come first and second in each electoral district. Often, but not always, these will be the candidates representing the Labor party and the Coalition (Liberal and National parties).
Virtual Ballot Box (VBB)	A data base corresponding to a physical ballot box in which the cast iVote® s are accumulated
Virtual Ballot Paper (VBP)	A blank or empty electronic ballot paper unique to each registration by a voter which is associated with the Credential Hash and available in the Core Voting System for electors to cast their vote.
Voting Centre	A venue where a NSWEC appointed election official supervises voting. These venues can either be either inside or outside NSW.
Ward	Subdivisions, with approximately equal numbers of electors, of a local government area.
Zero Knowledge Proof (ZKP)	Mathematical proof to demonstrate some property without disclosing certain private information. In this case, a ZKP is used to demonstrate that both encrypted votes have the same contents without actually decrypting them, i.e. the one to be stored in the ballot box, which is encrypted with the Election Public key, and the one to be sent to the Verification Server, which is encrypted with the Receipt Number and Random Extension have the same contents without actually decrypting them.

Appendix B – Legal, Operational and Technical Standards for e-Voting

Introduction

This appendix compares the iVote® system as implemented at the 2015 State General Election to the Committee of Ministers of the Council of Europe (CoE) Recommendation Rec(2004)11 on "Legal, Operational and Technical Standards for e-Voting" adopted on 30 September 2004[12]. More information about the CoE and e-voting can be found at their e-voting website[13].

The CoE recommendations are often used by countries evaluating e-voting systems. Recently Canada used the recommendations to evaluate the potential for using e-voting[14]. A similar comparison was done in the Norwegian trial election in 2011 by IFES[15].

The comparison conducted in this appendix showed that the iVote® system substantially complies with the recommendations. The areas of deviation are areas which for the most part are not addressed within the current electoral processes and are not considered significant with the NSW context.

[12] http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/Key_Documents/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf

[13] http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/

[14] http://www.elections.ca/content.aspx?section=res&dir=rec/tech/elfec&document=aa&lang=e

[15] http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic7_Assessment.pdf

CoE Recommendation	iVote® Compliance Statement	Compliance
Legal standards		
A. Principles		
I. Universal suffrage		
1. The voter interface of an e-voting system shall be understandable and easily usable.	iVote® is a comprehensible system which is easy for voters to use on both a phone and over the web using a computer or mobile device with a browser	Compliant
2. Possible registration requirements for e-voting shall not pose an impediment to the voter participating in e-voting.	iVote® has a simple and proven registration procedure.	Compliant
3. E-voting systems shall be designed, as far as it is practicable, to maximise the opportunities that such systems can provide for persons with disabilities.	iVote® has been designed with particular consideration for blind and low vision electors. An additional voting channel for disabled and elderly voters who have difficulty with technology are able to vote by talking to a call centre operator.	Compliant
4. Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.	The iVote® system is only available as an optional means of voting to eligible groups as defined by the enabling legislation.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
II. Equal suffrage		
5. In relation to any election or referendum, a voter shall be prevented from inserting more than one ballot into the electronic ballot box. A voter shall be authorised to vote only if it has been established that his/her ballot has not yet been inserted into the ballot box.	iVote® prevents an elector from inserting more than one ballot into the electronic ballot box. Revoting is allowed but only after the original vote has been deleted.	Compliant
6. The e-voting system shall prevent any voter from casting a vote by more than one voting channel.	Votes for postal and pre-poll channels are checked prior to the decryption of votes and duplicate iVotes are removed. An elector may have a duplicate ordinary vote in a polling place, however this is a known and accepted weakness of the current manual voting system. After decryption declaration votes which are duplicates of iVote® votes will be removed.	Partially Compliant
7. Every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once.	iVote® auditing procedures ensure all votes are counted	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
8. 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 correct result.	The NSWEC results management systems are capable of aggregating iVotes with other voting channels and reconciling results with votes issued	Compliant
III. Free suffrage		
9. The organisation of e-voting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.	iVote® extends suffrage to electors who otherwise would have difficulty voting independently or would have been unable to vote due to geographic constraints.	Compliant
10. The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection.	Voters have sufficient time to vote.	Compliant
11. Voters shall be able to alter their choice at any point in the e-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.	iVote® allows voters to change their vote at any point up to the time of submitting the vote. It even allows the elector to revote if they believe the vote did not reflect their intent or they were coerced.	Compliant
12. The e-voting system shall not permit any manipulative influence to be exercised over the voter during the voting.	iVote® like postal voting exposes the elector to manipulative influences. This is a risk which has been assessed and accepted. However it allows the elector to revote if they were coerced.	Partially Compliant
13. The e-voting system shall provide the voter with a means of participating in an election or referendum without	iVote® allows the casting of a blank ballot. This is the only form of informal ballot allowed.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
the voter exercising a preference for any of the voting options, for example, by casting a blank vote.		
14. The e-voting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed.	The iVote® voting interface clearly shows when the voting procedure has been completed. Also a verification process is provided which allows the elector to confirm that their vote was captured by iVote® as intended.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
15. The e-voting system shall prevent the changing of a vote once that vote has been cast.	iVote® does not allow the elector or any other person access to vote once it is cast. Votes can be removed from the ballot box but this is only when revoting occurs and is strictly supervised and reconciled to the registration system.	Compliant
IV. Secret suffrage		
16. E-voting shall be organised in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.	iVote® protects voter secrecy once the vote is submitted but as is the case with any unsupervised voting environment the secrecy of the vote at the time of voting is only controllable by the voter.	Partially Compliant
17. The e-voting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.	iVote® does not after decryption hold any information which could tie the voter to their vote. Encrypted ballots are stored using a double envelope strategy similar to that used for postal voting. The outer envelope consists of the voter's digital signature for the ballot, with the inner envelope being the encrypted vote. The outer envelope, with the ID credentials, is removed during the cleansing stage of the counting process. Ballots are then mixed, to make it impossible to determine the identity of the voter due to the order in which ballots are stored. The inner envelope, with the vote's value, is then decrypted at the final stage of counting where results are tabulated.	Compliant
18. The e-voting system shall be so designed that the	iVote® expects to take over 200,000 votes. This would average	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.	over 2,000 votes per electoral area. It is not possible to determine how someone voted with this number of votes.	
19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.	The voters secrecy cannot be breached as election officials only know how an elector voted if taking phone votes and then they do not know who the person was who voted. The vote preferences are not available to anyone until after the elector has been disconnected from the preferences during decryption.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
B. Procedural safeguards		
I. Transparency		
20. Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use.	iVote® awareness and general electronic voting promotion has been undertaken for the past two years and a general awareness campaign is planned for the election.	Compliant
21. Information on the functioning of an e-voting system shall be made publicly available.	A significant amount of material has been made available and will be expanded on up to the election.	Compliant
22. Voters shall be provided with an opportunity to practise any new method of e-voting before, and separately from, the moment of casting an electronic vote.	A practice system will be available for both phone and web based voting.	Compliant
23. Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishing of the results.	Several observer programs have been established and additional program of technical observers and decryption observers will be implemented.	Compliant
II. Verifiability and accountability		
24. The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.	The NSWEC has engaged a number of consultants to review the iVote® system and provide comment on any issues they have found.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
25. Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is working correctly and that all the necessary security measures have been taken.		Compliant
26. There shall be the possibility for a recount. Other features of the e-voting system that may influence the correctness of the results shall be verifiable.	All transactions of the system are captured in logs and available for audit. Recounting will involve rechecking all the security measures and the output from the system to ensure it has been correctly decrypted and tabulated.	Compliant
27. The e-voting system shall not prevent the partial or complete re-run of an election or a referendum.	A full backup of the system will be taken just prior to decryption and can be installed to allow the complete reprocessing of the votes in the event of a recount.	Compliant
III. Reliability and security		
28. The member state's authorities shall ensure the reliability and security of the e-voting system.	iVote® will operate out of a Tier 3 data centre and have full replication to a geographically separate site. Similar requirements apply for registration and verification components of the system.	Compliant
29. All possible steps shall be taken to avoid the possibility of fraud or unauthorised intervention affecting the system during	iVote® will be continuously monitored and all aspects of the system's operation will be logged and logs will be reviewed.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
the whole voting process.		
30. The e-voting system shall contain measures to preserve the availability of its services during the e-voting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.	iVote® will be protected from DDOS by a layer 3 and 4 filter placed in front of the webserver. The filter will only see encrypted traffic and as such will not be able determine the contents of the vote.. The phone system will be protected by the telecom provider. Availability will be addressed by response to item 28.	Compliant
31. Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the e-voting system is genuine and operates correctly.	iVote® is reviewed and tested before each event with standard set of procedures.	Compliant
32. Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods.	Access to systems is limited to nominated staff and access controls are tightly held. Key operations are done under supervision. In some cases such as with phone voting video capture is used when votes are taken by an operator and reviewed by a second operator.	Compliant
33. While an electronic ballot box is open, any authorised intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report, be monitored by representatives of the competent electoral authority and any	An auditor has been appointed to review all stages of the decryption process and provide a report at the end of the election.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
election observers.		

CoE Recommendation	iVote® Compliance Statement	Compliance
34. The e-voting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.	Votes are encrypted from the client system forward and not available to any other party.	Compliant
35. Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or referendum.	All voter information is stripped from the encrypted vote prior to decryption.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
Operational standards		
I. Notification		
36. Domestic legal provisions governing an e-election or e-referendum shall provide for clear timetables concerning all stages of the election or referendum, both before and after the election or referendum.	The Authorised procedures prepared for the election outline the timeline iVote® is to follow. These procedures have the force of legislation.	Compliant
37. The period in which an electronic vote can be cast shall not begin before the notification of an election or a referendum. Particularly with regard to remote e-voting, the period shall be defined and made known to the public well in advance of the start of voting.	iVote® is only implemented when an election event will occur. Registrations for iVote® will be taken before the issue of writs but these registrations are provisional on the writs being issued and an election event proceeding.	Compliant
38. The voters shall be informed, well in advance of the start of voting, in clear and simple language, of the way in which the e-voting will be organised, and any steps a voter may have to take in order to participate and vote.	iVote® will have an extensive advertising campaign targeted at the eligible elector groups prior to the commencement of voting starting once enrolment has commenced.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
II. Voters		
39. There shall be a voters' register which is regularly updated. The voter shall be able to check, as a minimum, the information which is held about him/her on the register, and request corrections.	NSW maintains a continuous roll which is used for the whole election and electors can check their registration details online. The Roll holds about 94% of the eligible electors.	Compliant
40. The possibility of creating an electronic register and introducing a mechanism allowing online application for voter registration and, if applicable, for application to use e-voting, shall be considered. If participation in e-voting requires a separate application by the voter and/or additional steps, an electronic, and, where possible, interactive procedure shall be considered.	The roll is used as the basis for registration of iVote® electors. iVote® electors have to satisfy additional eligibility criteria to use iVote®. This criterion is verified in a separate registration process. This process also obtains other electronic contact details.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
41. In cases where there is an overlap between the period for voter registration and the voting period, provision for appropriate voter authentication shall be made.	A second factor of ID is also obtained to ensure the elector's identity is correct. This is either a letter sent to the elector's enrolled address or they provide a drivers licence or passport number. Registration commences before the roll is closed and as such the electors registered at the time of roll close need to be revalidated against the closed roll. The electors removed are notified they are no longer registered to vote.	Compliant
III. Candidates		
42. The possibility of introducing online candidate nomination may be considered.	Online candidate nomination has been considered and at this time is not deemed to provide sufficient benefits to warrant pursuing. Problems relating to the payment of deposits by the close of the process add to the complexity of using online nominations.	Compliant
43. A list of candidates that is generated and made available electronically shall also be publicly available by other means.	All candidate details are published on the internet as soon as their nomination is finalised. Voice files are also provided on the internet to allow the candidates to confirm the pronunciation of their name for telephone voting.	Compliant
IV. Voting		
44. It is particularly important, where remote e-voting	A process of vote mark-off checking is done at the completion of	Partially

CoE Recommendation	iVote® Compliance Statement	Compliance
takes place while polling stations are open, that the system shall be so designed that it prevents any voter from voting more than once.	voting. This process compares online mark-offs which have accepted votes against iVotes prior to decryption. Those electors who have voted via another channel have their iVote® removed. This process suffers the same problem other declaration voting channels face in that election day votes using manual mark-off cannot be identified at the time of decryption so it is possible there will be duplication with some ordinary votes. Online mark-off in polling places will address this problem.	Compliant
45. Remote e-voting may start and/or end at an earlier time than the opening of any polling station. Remote e-voting shall not continue after the end of the voting period at polling stations.	iVote® is closed for new votes at 6pm on election day. This is consistent with practices in polling places. The electors in the system at that time are allowed to complete their vote.	Compliant
46. For every e-voting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote e-voting, such arrangements shall also be available through a different, widely available communication channel.	A telephone call centre and web based advisory services will be available.	Compliant
47. There shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote.	The user interfaces for all devices are reviewed prior to voting to ensure they provide a consistent and acceptable voting experience.	Compliant
48. The electronic ballot by which an electronic vote is cast shall be free from any information about voting options,	The electronic ballot closely represents the paper ballot and does not have additional information other than screen controls needed	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
other than that strictly required for casting the vote. The e-voting system shall avoid the display of other messages that may influence the voters' choice.	for voting.	
49. If it is decided that information about voting options will be accessible from the e-voting site, this information shall be presented with equality.	Information about voting options is not available from the voting site.	Compliant
50. Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election or e-referendum in which they are submitting their decision by electronic means is a real election or referendum. In case of tests, participants shall have their attention drawn explicitly to the fact that they are not participating in a real election or referendum and shall – when tests are continued at election times – at the same time be invited to cast their ballot by the voting channel(s) available for that purpose.	The training system has clear identification on it that the vote is for training only and is not a real vote. The real system is clear in that it states the vote is real and not for training and is the only vote the elector should make.	Compliant
51. A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.	The elector is able to verify their vote by calling the verification server which has an automated voice verifying preferences. The elector could record this message or provide their credentials to a third party. This weakness is similar to problems currently faced by postal voting.	Partially Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
52. In a supervised environment, the information on the vote shall disappear from the visual, audio or tactile display used by the voter to cast the vote as soon as it has been cast. Where a paper proof of the electronic vote is provided to the voter at a polling station, the voter shall not be able to show it to any other person, or take this proof outside of the polling station.	iVote® does not store any voting preferences on the client computer and the phone vote is not available from the voting system once the vote is completed.	Compliant
V. Results		
53. The e-voting system shall not allow the disclosure 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.	iVote® does not provide any results until the votes are decrypted which can only happen after the election is completed.	Compliant
54. The e-voting system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.	iVote® keeps all remote votes in one ballot box which is sufficiently large such that no electors vote can be determined.	Compliant
55. Any decoding required for the counting of the votes shall be carried out as soon as practicable after the closure of the voting period.	iVote® after close of poll verifies the elector has not multi voted and then decrypts the vote.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
56. When counting the votes, representatives of the competent electoral authority shall be able to participate in, and any observers able to observe, the count.	iVote® decryption ceremony will be conducted in the presence of scrutineers and official observers. Technical observers will assist in the decryption ceremony by simultaneously with the NSEWEC verify the votes held on the verification server match the votes decrypted from the core voting system.	Compliant
57. A record of the counting process of the electronic votes shall be kept, including information about the start and end of, and the persons involved in, the count.	iVotes® along with all other votes will be counted electronically. The votes without elector identification will be published showing their full preferences to allow the final count to be checked independently.	Compliant
58. In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such.	Should any irregularity be detected within iVote, either the entire pool of collected votes or just the affected votes can be recorded as such and prevented from entering the count, which occurs in a separate system.	Compliant
VI. Audit		
59. The e-voting system shall be auditable.	iVote® has extensive audit logging and has a voting protocol which implicitly allows the vote to be verified.	Compliant
60. The conclusions drawn from the audit process shall be applied in future elections and referendums.	iVote® uses a standardised audit process which is added to election to election.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
Technical requirements		
The design of an e-voting system shall be underpinned by a comprehensive assessment of the risks involved in the successful completion of the particular election or referendum. The e-voting system shall include the appropriate safeguards, based on this risk assessment, to manage the specific risks identified. Service failure or service degradation shall be kept within pre-defined limits.		
A. Accessibility		
61. Measures shall be taken to ensure that the relevant software and services can be used by all voters and, if necessary, provide access to alternative ways of voting.	Extensive accessibility testing is performed on the iVote® system to ensure that all voters can use it, whatever accessibility tools they use. There are also other voting channels of attendance, postal and pre-poll, which can be used in lieu of eVoting.	Compliant
62. Users shall be involved in the design of e-voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.	Users have been able to review a range of strategy and design documents and have input into the development of iVote. Users will be able to review the demonstration system.	Compliant
63. Users shall be supplied, whenever required and	iVote® interfaces are compliant with W3C standards.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
possible, with additional facilities, such as special interfaces or other equivalent resources, such as personal assistance. User facilities shall comply as much as possible with the guidelines set out in the Web Accessibility Initiative (WAI).		
64. Consideration shall be given, when developing new products, to their compatibility with existing ones, including those using technologies designed to help people with disabilities.	iVote® is intended for the use of disabled persons.	Compliant
65. The presentation of the voting options shall be optimised for the voter.	iVote® UI has been developed to optimise voter experience.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
B. Interoperability		
66. Open standards shall be used to ensure that the various technical components or services of an e-voting system, possibly derived from a variety of sources, interoperate.	Where possible iVote® has used open standards such as EML, SOAP and widely used technology platforms and tools.	Compliant
67. At present, the Election Mark-up Language (EML) standard is such an open standard and in order to guarantee interoperability, EML shall be used whenever possible for e-election and e-referendum applications. The decision of when to adopt EML is a matter for member states. The EML standard valid at the time of adoption of this recommendation, and supporting documentation are available on the Council of Europe website.	The EML standard has been adopted already within NSWEC and exchange of data from other systems within the organisation to the iVote® system uses EML, such as the EML 410 used for creating the ballots within iVote.	Compliant
68. In cases which imply specific election or referendum data requirements, a localisation procedure shall be used to accommodate these needs. This would allow for extending or restricting the information to be provided, whilst still remaining compatible with the generic version of EML. The recommended procedure is to use structured schema languages and pattern languages.	The iVote® system is a consumer of EML data from other NSWEC systems, which may have some localisation and would retain compatibility as per the recommendation.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
C. Systems operation		
(for the central infrastructure and clients in controlled environments)		Compliant
69. The competent electoral authorities shall publish an official list of the software used in an e-election or e-referendum. Member states may exclude from this list data protection software for security reasons. At the very least it shall indicate the software used, the versions, its date of installation and a brief description. A procedure shall be established for regularly installing updated versions and corrections of the relevant protection software. It shall be possible to check the state of protection of the voting equipment at any time.	iVote® will use configuration management to ensure software used is implemented at planned and is fully tested and compliant with specifications.	Compliant
70. Those responsible for operating the equipment shall draw up a contingency procedure. Any backup system shall conform to the same standards and requirements as the original system.	iVote® will have a completely separate replicated system as a redundant backup. Cut over to the redundant system will be manually triggered. Daily backups will be taken and kept for the requisite period then destroyed after the election retention period expires.	Compliant
71. Sufficient backup arrangements shall be in place and be permanently available to ensure that voting	iVote® will be monitored 24/7 during the election period. The contingency plans will be well documented and be reflected in the	Compliant

proceeds smoothly. The staff concerned shall be ready to intervene rapidly according to a procedure drawn up by the competent electoral authorities.	Approved Procedures.	
72. Those responsible for the equipment shall use special procedures to ensure that during the polling period the voting equipment and its use satisfy requirements. The backup services shall be regularly supplied with monitoring protocols.	iVote® will be hosted in a secure environment.	Compliant

73. Before each election or referendum, the equipment shall be checked and approved in accordance with a protocol drawn up by the competent electoral authorities. The equipment shall be checked to ensure that it complies with technical specifications. The findings shall be submitted to the competent electoral authorities.	iVote® will have a full audit plan which will be used to check system compliance before and after the election.	Compliant
74. All technical operations shall be subject to a formal control procedure. Any substantial changes to key equipment shall be notified.	iVote® will operate under strict configuration management procedures.	Compliant
75. Key e-election or e-referendum equipment shall be located in a secure area and that area shall, throughout the election or referendum period, be guarded against interference of any sort and from any person. During the election or referendum period a physical disaster recovery plan shall be in place. Furthermore, any data retained after the election or referendum period shall be stored securely.	iVote® Core Voting System will be housed in secure NSW government data centre. Other components of iVote® will be hosted in the NSWEC computer room or other secure private data centre.	Compliant
76. Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the competent electoral authorities, who will take the necessary steps to mitigate the effects of the incident. The level of incident which shall be reported shall be specified in advance by the electoral authorities.	iVote® Manager will be on call 24/7 during the election. Only the iVote® manager will be able to direct system changes in the event of a significant incident.	Compliant

D. Security		
I. General requirements		
(referring to pre-voting, voting, and post-voting stages)		
77. Technical and organisational measures shall be taken to ensure that no data will be permanently lost in the event of a breakdown or a fault affecting the e-voting system.	Backups and replication of systems will minimise the potential for data loss.	Compliant
78. The e-voting system shall maintain the privacy of individuals. Confidentiality of voters' registers stored in or communicated by the e-voting system shall be maintained.	The privacy of the voter's identity is maintained by not providing information during the registration process until the voter has identified themselves by providing information about themselves. In general terms the voter must provide all information with the exception of street number and postal address. The full address details is only provided after they correctly provide Name, DoB and street name.	Compliant
79. The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available.	The system is fully tested prior to it being used in a live election.	Compliant
80. The e-voting system shall 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	All access to the system other than public access requires two-factor identification. The second factor is physical and held by the user.	Compliant

authentication shall be effective before any action can be carried out.		
81. The e-voting system shall protect authentication data so that unauthorised entities cannot misuse, intercept, modify, or otherwise gain knowledge of all or some of this data. In uncontrolled environments, authentication based on cryptographic mechanisms is advisable.	Cryptographic mechanisms are used to store and transmit authentication data	Compliant
82. Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured.	The combination of iVote® number and PIN is sufficient to uniquely identify voters. Guessing of these numbers will cause the user to be blocked.	Compliant
83. E-voting systems shall generate reliable and sufficiently detailed observation data so that election observation can be carried out. The time at which an event generated observation data shall be reliably determinable. The authenticity, availability and integrity of the data shall be maintained.	iVote® will create log files for all election activity. The combination of verification evidence from the decryption process will provide evidence to support audit processes.	Compliant
84. The e-voting system shall maintain reliable synchronised time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observations data, as well as for maintaining the time limits for registration, nomination, voting, or counting.	iVote® uses multiple NTP servers to maintain reliable time.	Compliant
85. Electoral authorities have overall responsibility for compliance with these security requirements, which shall be	NSWEC has engage reputable consultants to review the	Compliant

assessed by independent bodies.	compliance of iVote® to security requirements.	
II. Requirements in pre-voting stages (and for data communicated to the voting stage)		
86. 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.	iVote® uses the same electoral roll used throughout the election. The roll integrity is checked on loading into iVote.	Compliant
87. The fact that candidate nomination and, if required, the decision of the candidate and/or the competent electoral authority to accept a nomination has happened within the prescribed time limits shall be ascertainable.	The nomination process happens independently of iVote® and is considered to be satisfactory.	Compliant
88. The fact that voter registration has happened within the prescribed time limits shall be ascertainable.	The enrolment of voters happens independently of iVote® and is considered to be satisfactory. The registration of eligible voters for iVote® is done through a purpose built registration system which creates the credentials necessary to vote. The registration process closes prior to the close of the poll.	Compliant
III. Requirements in the voting stage (and for data communicated during post-election stages)		
89. The integrity of data communicated from the pre-voting stage (e.g. voters' registers and lists of candidates)	Data used to register electors and candidates is the same data used in the remainder of the election process. The data as loaded	Compliant

shall be maintained. Data-origin authentication shall be carried out.	and used in iVote® is characterised and these parameters are compared to the source data.	
90. It shall be ensured that the e-voting system presents an authentic ballot to the voter. In the case of remote e-voting, the voter shall be informed about the means to verify that a connection to the official server has been established and that the authentic ballot has been presented.	iVote® registration system advises the voter of the valid URL used to vote. Should this URL not be presented to be voter they should abort the process.	Compliant
91. The fact that a vote has been cast within the prescribed time limits shall be ascertainable.	The date and time of submission of each vote is recorded	Compliant
92. Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that could modify the vote.	The main protection against tampering is the verification of the vote using an independent second channel i.e. voice over a phone	Compliant
93. Residual information holding the voter's decision or the display of the voter's choice shall be destroyed after the vote has been cast. In the case of remote e-voting, the voter shall be provided with information on how to delete, where that is possible, traces of the vote from the device used to cast the vote.	iVote® generates the vote in JavaScript and does not store it on the local device. The vote verification uses a dynamically created voice file and as such there is not residual information available after the verification. The votes themselves are removed from the encrypted votes and other data on the server is stored after the election and destroyed once the retention period lapses. The final votes in the clear are published.	Compliant
94. The e-voting system shall at first ensure that a user who tries to vote is eligible to vote. The e-voting system shall authenticate the voter and shall ensure that only the appropriate number of votes per voter is cast and stored in	iVote® uses a unique set of 8 and 6 digit numbers to determine the identity of the person voting. This approach when coupled with entry restrictions on the user interface is sufficient to allow the person voting to be uniquely identified to the system as an eligible	Compliant

the electronic ballot box.	voter but not as a person.	
95. The e-voting system shall ensure that the voter's choice is accurately represented in the vote and that the sealed vote enters the electronic ballot box.	iVote® uses a two-step verification process to ensure that the voter's choice is accurately represented in the vote stored in the Electronic ballot box. The first step is to allow the voter to verify that vote as cast is the vote that is stored by providing a feed-back of the vote stored via a second channel. The second is to check that the votes stored are the votes decrypted and sent to the count.	Compliant
96. After the end of the e-voting period, no voter shall be allowed to gain access to the e-voting system. However, the acceptance of electronic votes into the electronic ballot box shall remain open for a sufficient period of time to allow for any delays in the passing of messages over the e-voting channel.	iVote® will close access to the system at the close of poll but will allow voters in the system time to reasonably complete their votes. This is similar arrangement to the processes in a polling place.	Compliant
IV. Requirements in post-voting stages		
97. The integrity of data communicated during the voting stage (e.g. votes, voters' registers, lists of candidates) shall be maintained. Data-origin authentication shall be carried out.	iVote® will maintain logs of the voting and registration transactions until the retention period of the election is passed.	Compliant
98. The counting process shall accurately count the votes. The counting of votes shall be reproducible.	iVote® publishes all the votes to be counted in the clear allowing anyone who can write a program to perform their own count.	Compliant
99. The e-voting system shall maintain the availability and integrity of the electronic ballot box and the output of	iVote® will maintain the electronic ballot box transactions until the	Compliant

the counting process as long as required.	retention period of the election is passed.	

CoE Recommendation	iVote® Compliance Statement	Compliance
E. Audit		
I. General		
100. The audit system shall be designed and implemented as part of the eVoting system. Audit facilities shall be present on different levels of the system: logical, technical and application.	iVote® auditing is mandatory and requires audit facilities to be present for all phases of voting. Auditing will cover people, process and technology.	Compliant
101. End-to-end auditing of an e-voting system shall include recording, providing monitoring facilities and providing verification facilities. Audit systems with the features set out in sections II – V below shall therefore be used to meet these requirements.	iVote® will provide detailed logging and which will provide monitoring for the election. It will also provide an independent verification facility for elections and verification of the final decrypted votes.	Compliant
II. Recording		
102. The audit system shall be open and comprehensive, and actively report on potential issues and threats.	The auditor will prepare a report which will outline all the issues identified during the election which could have been as threat to the integrity of the electoral process.	Compliant
103. The audit system shall record times, events and actions, including:	Extensive logging is built into the iVote® system as follows	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
a. 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.;	All noted information and more is captured in the logs for iVote®	Compliant
b. any attacks on the operation of the e-voting system and its communications infrastructure;	iVote® will be monitored using Network and Systems Operation Centre.	Compliant
c. system failures, malfunctions and other threats to the system.	System failures and malfunctions will be captured and independently assessed by the auditor.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
III. Monitoring		
104. The audit system shall provide the ability to oversee the election or referendum and to verify that the results and procedures are in accordance with the applicable legal provisions.	The iVote® auditor will assess the operation of the election against the relevant legislation.	Compliant
105. Disclosure of the audit information to unauthorised persons shall be prevented.	Audit reports will be made public but the source information will be restricted depending on the sensitivity of the information from a privacy and security perspective. Also the protection of intellectual property will be considered in this decision.	Compliant
106. The audit system shall maintain voter anonymity at all times.	iVote® is unable in the normal course of operation to connect the elector to their vote in the clear. Even a person who illegally obtained data with sufficient detail to do this would need significant skill and resource to attempt this task.	Compliant
IV. Verifiability		
107. The audit system shall provide the ability to cross-check and verify the correct operation of the e-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.	iVote® audit system is designed to provide elector's a means of verifying of their vote as cast and then the auditor is able to verify all votes as captured are the same as the vote that was decrypted.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
108. The audit system shall provide the ability to verify that an e-election or e-referendum has complied with the applicable legal provisions, the aim being to verify that the results are an accurate representation of the authentic votes.	In so much as the legislation provides for the verification of votes the iVote® system is able to verify the vote as cast is the vote as counted. iVote® achieve this by verifying each stage of the voting process. While the current manual system can only try and prove good chain of custody, it cannot prove the final count matches the votes as cast.	Compliant
V. Other		
109. The audit system shall be protected against attacks which may corrupt, alter or lose records in the audit system.	iVote® uses immutable logs to protect the audit system records against tampering.	Compliant
110. Member states shall take adequate steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed.	Persons involved in the management and audit process will be required to sign agreements which ensures they are aware of their legal responsibilities.	Compliant

CoE Recommendation	iVote® Compliance Statement	Compliance
F. Certification		
111. Member states shall introduce certification processes that allow for any ICT (Information and Communication Technology) component to be tested and certified as being in conformity with the technical requirements described in this recommendation.	In so much as applicable certifications exist for iVote® components certification will be undertaken. Most certification however will rely on the manufacturer's compliance statement.	Compliant
112. In order to enhance international co-operation and avoid duplication of work, member states shall consider whether their respective agencies shall join, if they have not done so already, relevant international mutual recognition arrangements such as the European Co-operation for Accreditation (EA), the International Laboratory Accreditation Co-operation (ILAC), the International Accreditation Forum (IAF) and other bodies of a similar nature.	Not Applicable	N/A