NSW Electoral Commission


# NSW Electoral Commission
# iVote Project

# Code Review Report

# Version Control

| Version No | Date | Who | Comments | Review |
|---|---|---|---|---|
| V0.1 | 22 Jul 19 | TB | Initial draft | |
| V1.0 | 29 July 19 | | Final approved version | |
| | | | | |
| | | | | |

# Contents

# 1 Introduction

Demtech Group conducted a review of iVote source code with the following objectives:

- Assessment of extent the source code implements the voting protocol
- Identify issues with the source code that could endanger the availability of the software during the election period
- Assessment of extent that the system delivers integrity of the election, security requirements are appropriately implemented to preserve secrecy of the vote.
- Published the report to deliver transparency even though the code may be subject to non-disclosure
- Provide suggestions and recommendations (if necessary) regarding implementation improvements.

The scope of the review was the iVote Voting and Assurance System application software delivered by Scytl.

Demtech provided a written report on the findings of the review which is provided as an embedded PDF in Attachment A. Scytl's response to the findings is similarly included in Attachment B.

The document covers the NSWEC's response to the review findings and is aimed at a non-technical audience; however, the appendix does contain a somewhat more technical response.

An overview of the iVote® System[1] is provided here: https://www.elections.nsw.gov.au/About-us/Reports/iVote-reports.

[1] 1 Registered trade mark of the State of NSW (New South Wales Electoral Commission).

# 2 Executive Overview

Demtech used a variety of techniques to review the code. They used automated code scanning tools to identify vulnerabilities, bugs, and possible bad programming style. They analysed the code to compare the accuracy of the implementation to the software specifications. And they also sampled coverage analyses to assess the effectiveness of the testing regime.

Demtech concluded that the overall quality of the code was in general high, and that the implementation was largely free from bad and insecure programming patterns. They identified an area of the code that was part of the back office post-election processing which was still under development and was an exception to the general high quality.

Demtech raised seven observations and three recommendations which NSWEC have responded to below. Demtech presented the detailed findings of their review and highlighted ten items in particular to draw to NSWEC's attention in the areas of potential bugs, possible security issues as well as programming styles and techniques.

NSWEC considered Demtech's report carefully and concluded that, while there were items raised that needed attention, there weren't any issues of sufficient gravity that would preclude using the software in the State General Election.

Scytl were sent Demtech's report at the time. They subsequently provided NSWEC with responses to the technical points found in Demtech's review. Scytl noted that the findings have been considered in the version of the voting system used for the 2019 election and others to be taken into account for future releases of the system. On a number of points, Scytl provided additional information to address the issues raised.

NSWEC reviewed Scytl's response to ensure issues were/will be adequately addressed and that there was clarity in the response.

# 3 NSWEC response to issues raised in Demtech's report

The section is organised in alignment with Demtech's, so there is one subsection covering each section in the report. The section is written in the form of supplementary notes to the reports in appendix A and B. Appendix B is written in the form of supplementary information to Appendix A.

The section contains responses to all the points raised in the executive summary. In the other areas, there are only responses to items which warrant information to the response provided by Scytl.

## 3.1 Executive Summary

| Demtech Comment | NSWEC Response |
|---|---|
| Observation 1: TODO Comments | NSWEC considered Demtech's report carefully and concluded that, while there were items raised that needed attention, there weren't any issues of sufficient gravity that would preclude using the software in the State General Election. |
| Observation 2: Design Document Quality | We continue to provide comments to Scytl on design documentation. In general the Scytl documentation is comprehensive and they act on feedback. |
| Observation 3: Unused functionality | The NSWEC stated in its procurement strategy that "The intent … is to use off-the-shelf software wherever possible. Where off-the-shelf software is used, NSWEC will try to minimise customisation whilst ensuring that the software fully meets the NSWEC requirements." Also, refer to section 2.2 in Scytl's response. |
| Observation 4: different ivapi library versions for voting and verification | Scytl identified the ivapi library version included in each release. NSWEC deployed a common ivapi library version for voting and verification throughout testing and for the election. |
| Observation 5: documentation gap concerning entropy in the JavaScript client. | See section 2.6 of Scytl's response. |
| Observation 6: source code genealogy | See response to observation 3. |
| Observation 7: library dependencies | NSWEC uses the CVE database, amongst other sources and methods, to identify vulnerabilities. |
| Recommendation 1: Design Documentation | See response to Observation 2. |
| Recommendation 2: Source code refactoring | Refer to section 2.2 in Scytl's response. |
| Recommendation 3: Source code build | NSWEC will consider this item when engaging third parties for code reviews in the future. |

## 3.2 Scope and Review Methodology

| Demtech Statement/ Comment | NSWEC Commentary |
|---|---|
| Referenced documents | Internal reference documents have been redacted.<br>A later version of the Voting Protocol Description will be published by NSWEC which includes adjustments to align the description with details of the implementation. |

## 3.3 Major Findings

| Demtech Comment | NSWEC Commentary |
|---|---|
| Client Side – obtaining de-obfuscated code | NSWEC will consider requesting de-obfuscated code to be provided to code reviewers in the future. |
| Misuse of the Voting App | NSWEC plan to investigate improvements to detecting misuse in the future. |
| Entropy and randomness in the Javascript client | Demtech's comment on NSWEC acquiring copies of entropy assessments noted. |
| Potential Overflow [in mixing] | Mixing of the encrypted votes, to sever the link to the voter, takes place on an air-gapped server with restricted access. The requirement for voting was to support up to 1 million voters. |
| Secret Key Reuse | NSWEC follows a process for deleting the secret key shares as part of the post-election clean-up process. |

## 3.4 Detailed Findings

| Demtech Comment | NSWEC Commentary |
|---|---|
| 6.2.6 Cleansing<br>"Cleansing software independence" | During the cleansing process, which is subject to scrutiny, a list of voter identifiers allocated and removed is extracted from the Credential Management System and compared to voter identifiers in the Voting System ballot box |

## Attachment A – Demtech's Report

Published here https://www.elections.nsw.gov.au/About-us/Reports/iVote-reports

## Attachment B – Scytl's Response

Published here https://www.elections.nsw.gov.au/About-us/Reports/iVote-reports