

## **Part 2**

# Work of the Commission



## **2.1 Introduction**

This part describes the work of the Commission in its review of the chosen electronic voting system and related matters, including the procedures and documentation governing its use at elections.

The hardware and software components were examined both as individual items and as a whole system with design and other relevant issues being considered in each case. The previous tests of the system listed at *Appendix 1B* were reviewed and the Commission decided that further tests should be carried out, including an examination of the source code.

Documented procedures for the use of the system, including those relating to storage and transportation, were also reviewed from the different viewpoints of auditors and election practitioners and a number of changes to procedures and the introduction of new controls were recommended. A risk analysis of the system was carried out and its secrecy and security aspects were reviewed.

The system was considered in the light of international experience of electronic voting, including in countries where a system designed by the same manufacturers has been used previously, and in light of its previous use in Ireland.

The work carried out by and on behalf of the Commission is merely summarised in this part and the full details and results of each strand of the work are set out in the relevant part of *Appendix 2* as indicated in each case. The Commission's analysis, observations, conclusions and recommendations arising from the work are set out in *Parts 4, 5 and 6* of this report.

## **2.2 Structure of this Part**

This part describes the work of the Commission in three main categories: Review of the System (*section 2.3*); Review of Procedures, Documentation, Risk, Secrecy and Security (*sections 2.4 to 2.7*); Review of International Experience and Other Issues (*sections 2.8 and 2.9*).

*Section 2.3* of this part containing the Review of the System is further divided into subsections dealing with Hardware Evaluation, Software Evaluation and System Evaluation. Each subsection in turn is further divided into paragraphs relating to (a) Review of Previous tests (b) Further Tests Carried Out, (c) Review of Design and further paragraphs (d), etc. containing additional matters as appropriate in each case.

## **2.3 Review of the Electronic Voting System**

The Commission obtained samples of the various hardware and software components of the system from the Department of the Environment, Heritage and Local Government. Reports of previous tests carried out on the system were reviewed and further tests were carried out by the Commission. For the purposes of this summary, the hardware and software elements of the system are dealt with separately from each other and from the system as a whole.

***Hardware Evaluation*****(a) Review of Previous Tests**

Tests carried out on the hardware elements of the system by PTB, Zerflow, TNO and KEMA were reviewed and assessed for quality and comprehensiveness as described at *Appendix 2A*. It was concluded that, while the voting machine itself had been comprehensively tested, the programming and reading unit had not been tested.

Queries were raised with PTB in relation to the results of its testing of various hardware elements of the system against the specified requirements<sup>4</sup> for voting machines for use at elections in Ireland. The replies by PTB to these points are included in the report set out at *Appendix 2B*.

The report at *Appendix 2C* draws attention to a number of issues arising from the PTB tests of the voting machine, including the absence or usefulness of error messages for machine operators, concerns about machine security and identification and the inadvertent deletion of backup data.

None of the test reports reviewed by the Commission related to the hardened PC and printer provided to returning officers for use exclusively in running the election management software.

**(b) Further Tests Carried Out**

Tests were carried out on the voting machine as configured by the insertion of a programmed ballot module. These tests confirmed that the buttons used by voters to select preferences corresponded to the correct candidate details programmed on the module and that the printouts produced by the machine before and after a poll were correct.

The functionality of the ballot module in recording votes (as indicated by printouts from the voting machine at the opening and the closing of the poll) was tested. It was noted that, while no votes could be added to modules following the close of poll and printout, it was possible to cast votes before the open-poll printout occurred.

In a separate test, modules containing voting data were exposed to an intense electromagnetic field and were found to have retained their data accurately. These tests are described at *Appendix 2D*.

An “input-output” test was carried out on a sample of the voting machines deployed to returning officers throughout the country. In the course of this exercise, 739 voting machines were tested, together with a corresponding number of ballot modules. Further details of this test are set out below under *System Evaluation* and the test is described in full at *Appendix 2C*.

---

<sup>4</sup> Requirements for Voting Machines for Use at Elections in Ireland (Department of the Environment, Heritage and Local Government DVREC-2, 5 March 03)

(c) Review of Hardware Design

The Commission did not obtain access to the wiring diagrams and schematics for the voting machine, the ballot module or the programming reading unit. It was therefore not possible to evaluate and comment on the formal design of these devices. However, observations based on a physical examination of the system components, together with an examination of the hardened PC are included in the reports at *Appendices 2B, 2C and 2D*.

It was noted in relation to the voting machine that, while the casting of a blank vote is prohibited when the machine is configured for a single election, it is possible to vote in one election while not voting in others when the machine is configured for multiple elections. These tests are also described at *Appendix 2D*.

The report at *Appendix 2C* highlights a number of usability issues concerning the voting machine as considered from both the voter's perspective and the poll worker's perspective and commenting in particular on physical set-up, display and interface features, disabled access and use of the remote console.

### ***Software Evaluation***

(a) Review of Previous Tests

Previous desk reviews of the election management software carried out by Nathean Technologies and reports of previous tests of the counting software carried out by ERS were assessed as described at *Appendix 2A*. It is concluded that, while the counting module of the IES had been tested, additional testing is required. It is also concluded that desk reviews are not an adequate alternative to comprehensive testing for such a large piece of software and that additional testing of the IES software as a whole is therefore desirable.

The report at *Appendix 2A* also highlights the fact that, while the election management software has been desk reviewed, no independent testing has been carried out on its functions in relation to the disaggregation (at multi-ballot elections) and aggregation of the votes after they are read in from individual modules, the encryption of votes onto a CD for transfer to different count centres at multi-ballot elections and the mixing of the votes prior to counting.

A further commentary at *Appendix 2B* on the desk reviews and testing of the software draws attention to an apparent error in the pseudo code (but potentially reflecting a corresponding error in the actual code) used in a desk review to describe the function of the actual code in the transfer of surpluses and to a rounding error detected in the course of testing of the count software carried out in February 2004.

The report at *Appendix 2C* also notes a number of additional issues arising from the test reports and desk reviews of the source code for the software.

**(b) Further Tests Carried Out**

Parallel testing of the counting software was carried out by the Commission using published voting data. A new counting program known as the “Coyle-Doyle Implementation” was developed and the votes recorded at three constituencies in the pilot tests carried out at the 2002 Dáil general election were counted using both counting systems in parallel. The same results were obtained under both systems, confirming that the votes at these elections were counted correctly by the version of the software used at the time.

Further parallel tests were carried out on both systems using large numbers of randomly generated data sets together with data sets designed to give rise to “difficult” or “unusual” counting scenarios. The results produced by the count software and the Coyle-Doyle Implementation agreed in approximately 99.9% of cases. In the remainder of cases tested, the variations in results were caused by the manner in which the count software used floating point numbers during surplus transfers to determine the transfer of whole votes, in certain circumstances causing errors in surplus distribution. Details of these parallel tests are set out at *Appendix 2E*.

The Commission did not obtain access to the source code for the embedded software on the voting machine. Furthermore, as the manual entry of votes through the machine’s user interface is labour intensive and time consuming, it was not possible to carry out extensive testing on the voting machine using large data sets. However, the sample test carried out on 739 voting machines represents an effective “black box” test of the embedded software on the voting machine using a single large data set of sample votes. Further details of this test are set out below under *System Evaluation* and the test is described in full at *Appendix 2C*.

**(c) Review of Software**

The report at *Appendix 2B* expresses concern that new versions of the election management and counting software continue to be submitted for review and testing so close to an election. Particular mention is made of the importance of reviewing and testing each new software version in full as errors can arise in older parts of the code when newer parts reference them in unexpected or incorrect ways.

The degree to which the design, development, review and testing of the software have been carried out in accordance with recognised software assurance methodologies is also discussed in *Appendix 2B*, concluding that there is insufficient evidence, from the tests carried out and other system documentation available to the Commission, to establish that such methodologies have been implemented in the case of the chosen system.

The report at *Appendix 2C* deals with the ease of installation of the software on the hardened PC and outlines a number of usability issues with the operating procedures and user interface of the software.

It was noted, in particular, that different versions (including older versions) of the software could be loaded and reside simultaneously on the hardened PC as described at *Appendix 2D*.

(d) Software Assurance

The Commission received expert advice concerning the importance of software assurance, namely, establishing that software can be trusted to perform according to its functional specification and that it does not have any undesirable behaviour. The advice received by the Commission indicated that access to the source code would be essential in establishing the trustworthiness of the software.

The Commission has noted that, as the system is self auditing and does not provide a facility for independent audit of the process for the recording of votes, the requirement for a full source code review is heightened significantly on account of the need to establish that no unexpected behaviour of the system will occur that cannot be identified by means of “black box” testing.

It was also indicated to the Commission that, while the comprehensive inspection and testing process that would be necessary to evaluate the source code, comprising up to 300,000 lines of code, could not be carried out within the scope of the timeframe of this report, some useful deductions and inferences could be made from a preliminary review of the code in the short term.

The Commission accordingly sought, through the Department of the Environment, Heritage and Local Government, to obtain access to the full source code of the system, namely the election management module, the vote counting module and the embedded software on the voting machine, together with the wiring diagrams and schematics for the various hardware devices.

The Commission was advised by the Department that, because a section of the software relating to Presidential elections remained under development by the manufacturers, the source code had, as yet, neither been purchased nor acquired under licence by the State and it was therefore necessary for the Commission to approach the manufacturers directly in relation to obtaining access to it.

While the manufacturers declared that they were anxious to cooperate with the Commission in this matter, it was not possible within the timeframe of the Commission’s report due on 1 May 2004 to reach agreement on the terms as to accreditation, confidentiality and liability under which the full code would be released for third-party inspection on behalf of the Commission.

(e) Review of Source Code

Although it was not possible for the Commission to obtain access to the full source code of the system, the source code for the vote counting module of the software was released in time to allow a preliminary inspection to be carried out on behalf of the Commission.

The vote counting module gives expression to the rules for the counting of the votes at Irish elections and referenda as set out in various statutes and is thus effectively unique to Ireland.

The vote counting module comprising of the order of 100,000 lines of code was accordingly reviewed on behalf of the Commission. However, in view of the terms under which the code was released for review, it is not possible for the Commission to publish the results of the inspection although they have been taken into account by the Commission in reaching its overall conclusion.

***System Evaluation*****(a) Review of Previous Tests**

In addition to the live pilot tests of the system carried out at the 2002 Dáil general election and referendum, further tests of the system are understood to have been carried out by the Department of the Environment, Heritage and Local Government based on data from local elections held at Athy and Buncrana in 1999. However, from the test results available to the Commission, it appears that no independent “end-to-end” testing of the system has been carried out.

**(b) Further Tests Carried Out****Vote Gathering**

In an “input-output” test of the system carried out by the Commission, 739 voting machines were randomly selected for testing from the 6972 machines assigned to returning officers throughout the country. Ballot modules were programmed with the details of a European election and each was inserted into a voting machine with an appropriate ballot paper being printed and placed on the voters’ panel of the machine. Fifty pre-determined votes were then entered on each voting machine and the preferences entered in each case were noted and authenticated by two persons before the vote was cast. In a further complementary test, the manual entry of 5000 such votes was video recorded to establish the error rate attributable to incorrect data input and other factors.

The ballot modules from all 739 machines, corresponding to an electorate of 36,950 voters, were returned to a central location, and the recorded votes were then compared with the input votes as described at *Appendix 2C*.

**Vote Counting**

The Commission also carried out an end-to-end test of the system by conducting a miniature election to simulate the use of the system at the European and local elections due to be held in June. This test involved the configuration and use of the system in the casting and counting of votes in simultaneous polls at European, local and town council elections as described at *Appendix 2D*.

**2.4 Review of the Procedures and Documentation for Electronic Voting**

The procedures governing the use of the electronic voting system are complementary to the functioning of the system itself and can thus have a bearing on its secrecy and accuracy.

The Commission accordingly reviewed the system operation manuals prepared by the manufacturers and the procedural guidelines for the conduct of elections, including as regards use of the system, issued to returning officers and other election personnel by the Department of the



Environment, Heritage and Local Government. The purpose of this review was to assess the control procedures surrounding the use of the system, to identify any areas of risk which may exist and to suggest how these risks can be addressed.

This work was approached from two similar perspectives. A formal review of the procedures was carried out from the standpoint of an independent auditor and by reference to best practice criteria while a separate review, also from an audit standpoint, but drawing on the practical expertise and knowledge of a group of persons experienced in the conduct and administration of a range of election types in Ireland was also carried out.

Procedures for the storage, transportation, deployment and use of the system were accordingly reviewed, areas of risk were identified and recommendations made as regards additional controls and procedures.

Both reviews recommend changes and additions to the procedures for the use of the system and to the documentation provided to election personnel, some of which remained under preparation by the Department of the Environment, Heritage and Local Government at the time of the Commission's interim report.

The detailed work of these reviews is set out at *Appendices 2F* and *2G*. In addition, the report at *Appendix 2C* includes a review of the procedures for the installation and use of the election management software.

## **2.5 Risk Analysis**

In addition to the general audit of controls and procedures outlined above, a formal risk analysis of the chosen system as it would operate at elections was carried out on behalf of the Commission. By reference to the system itself and the administrative and other electoral procedures surrounding it, a range of possible undesirable events was identified and described. The probability of each event was estimated and an assessment made of its impact. Finally, any pre-emptive or corrective steps that could be taken to reduce or eliminate the probability of occurrence or to recover in the event of occurrence were identified.

The risk analysis identified 5 material risks in connection with the use of the system at the June elections:

- error in the system as a whole;
- error in voting machine software affecting all machines;
- tampering with software to alter election result;
- tampering with ballot modules during transportation;
- damage to machines before elections.

The first two risks are relevant to the work of the Commission in relation to the system itself, particularly as regards the adequacy of system testing and the trustworthiness of the software, while the remaining three risks are relevant to the Commission's work in relation to the procedures for the deployment and use of the system. The analysis concluded that, while the procedural risks could be reduced or eliminated in advance of the June elections, there was not sufficient time before the June elections to deal with the risks inherent in the use of the system itself.

It was also noted that a number of risks associated with the current paper voting system are eliminated by electronic voting, including inadvertently spoiled votes, misreading of votes in counting, misclassification of votes by returning officers and inaccuracies in count results attributable to the latter two factors.

The results of the risk analysis reflect many of the specific concerns expressed in the public submissions received by the Commission and which are discussed in *Part 3*. In particular, the analysis offers a useful tool with which to evaluate the materiality of the risks giving rise to these concerns in terms of both their likelihood of occurring and their impact if they do occur. Full details of the risk analysis are set out at *Appendix 2H*.

## **2.6 Secrecy of the Ballot**

Although a significant focus of the Commission's work was on the testing of the system, principally with a view to verifying its accuracy in the recording and the counting of the votes, the Commission also sought to have a review undertaken of the specific secrecy issues, if any, associated with the use of the system.

The review set out at *Appendix 2I* concludes that, subject to the implementation of appropriate procedures, the system represents no increased risk to the secrecy of the ballot for ordinary voters but that there is a risk in a number of special circumstances including the following:

- publication of the votes cast may lead to voter identification either in circumstances of small polling centres or where voters have been pressurised or intimidated into recording a lower preference "signature" to indicate how they have voted;
- re-keying of postal and special voters' votes and the increased need for assistance in the case of some disabled voters may involve a reduction in secrecy for these voters;
- where the voter does not cast a vote, whether deliberately or in circumstances where they have expressed preferences with the intention of voting but have overlooked pressing the "cast vote" button, the operator will be aware of this fact (but not of the preferences expressed) and will have to reset the machine for the next voter.

The review also concluded that the "beeps" made by the machine when the voter makes an error may give rise to mild embarrassment but will not diminish the secrecy of their vote. However, the Commission has noted that the machine also "beeps" (with a different sound) when preferences are being expressed by voters and that the number of "beeps" may thus be used to make limited inferences as to the number of preferences expressed, even if not disclosing the actual choices made in each case.

While the Commission had already determined that the secrecy entitlements of persons wishing to record a null vote was beyond its definition of secrecy of the ballot, the outcome of this review served the useful purpose of confirming that there were no other secrecy issues which had not already come to the attention of the Commission by other means in the course of its work.

## **2.7 Security**

### ***Security at Elections***

Under the current system of paper voting, members of an Garda Síochána attend at polling and counting centres while votes are being cast and counted and they participate in the transportation and custody of ballot boxes between centres. The investigation of alleged electoral offences is also a matter for an Garda Síochána.

It was of interest to the Commission to establish whether and how the security aspects of elections and the opportunities for criminal activity, particularly as regards computer fraud, were likely to be affected by the introduction of electronic voting.

Members of an Garda Síochána were therefore invited to examine the electronic voting system and the procedures for its use and to participate in the evaluation of its security aspects. The views of an Garda Síochána on these matters were accordingly reported to the Commission and, while they remain confidential to the Commission, they are reflected in its conclusions and recommendations as set out in this report.

### ***System Security Policy***

A discussion of the security requirements specified for the system in the context of recognised security standards is contained in *Appendix 2B*. It is concluded that security features of the system outlined in the published statements<sup>5</sup> are self-defining instead of being measured against internationally recognised criteria and that such criteria appear to be absent from the original specification for the system.

### ***Third Party Interference***

The reports at *Appendices 2B* and *2C* also highlight a number of areas in which the system components might be vulnerable to third party interference. The threats considered include some deceptions of lesser likelihood in relation to the use of the voting machine but also threats to its internal components and software, and physical threats to the ballot modules and the hardened PC.

### ***Physical Security***

The set of two colour-coded keys for the operation of the programming reading unit (which programs and reads the ballot modules before and after the poll respectively) are understood to be common to all machines and are thus interchangeable. This is stated by the manufacturer to be a function of the simplicity of the system leading to its ease of use.

While the provision of unique keys for each machine would undoubtedly present its own difficulties on polling day, the use of common key sets clearly lends itself more readily to situations where it is

---

<sup>5</sup> Security and Audit Features of the Election Management System (Department of the Environment, Heritage and Local Government, January 2004)

sought to subvert or influence the outcome of the election by either interfering with a number of programming reading units or by obtaining one for the purpose of programming or reading one or more ballot modules without authority.

A further issue concerning the use of these key sets is described at *Appendix 2D*. As both keys are required to be turned on in order to use either the programming or the reading slot on the programming reading unit, there is no physical distinction (apart from the slot used) between the configuration of the keys when programming and when reading ballot modules. It is suggested that this could lead to inadvertent overwriting of a ballot module.

The reports at *Appendices 2B* and *2D* describe how it was found possible to bypass physical and electronic security measures implemented in respect of the “hardened” PC and then to overwrite or modify the software.

### ***Custody and Transport***

In view of the significant issues which can arise through unauthorised access to voting machines and other equipment and software used for electronic voting, it is of vital importance that there are correspondingly substantial procedures and controls in place to minimise the likelihood of such access, both at election time and between elections. This requirement is accentuated by the fact that voting equipment is stored at numerous different locations around the country.

The requirements for enhanced procedures and controls in this area (and for these to be fully and clearly documented) are discussed in the reviews of documentation and procedures described at *Appendices 2F* and *2G* and relate to issues surrounding the manufacture, transport, custody, deployment and use of the equipment, both at and between elections.

## **2.8 International Experience of Electronic Voting**

Although the international experience of electronic voting in general can have no direct bearing on the secrecy and accuracy of the chosen system in an Irish electoral context, the Commission found it useful to consider the range of issues that have arisen as regards the implementation of electronic voting using different systems in other jurisdictions.

The Commission accordingly carried out a summary review of the experience in countries where electronic voting has been implemented either substantively or on a trial basis while the experience of the use in the Netherlands and Germany of a voting machine supplied by the same manufacturer was reviewed separately and in greater detail.

### ***Experience in Other Countries***

The report at *Appendix 2J* reviews the experience of electronic voting, principally in elections at national level, using a variety of different systems in a wide range of countries. Although electronic voting is found to be a relatively uncommon practice worldwide, there appears to have been neither widespread negative reaction to it nor evidence of significant errors or system failures in its use.

The motivations for the move towards electronic voting in other countries have included the

objective of eliminating inaccuracies and errors inherent in the use of the paper system, particularly under complex voting rules such as those in Ireland.

Useful conclusions from this report include the relative merits of pilot testing and parallel testing in a live electoral environment and how issues of public confidence can be addressed through the publication of source code and through the design of systems using open-source software.

### ***Experience in the Netherlands and Germany***

The report at *Appendix 2K* reviews the experience of electronic voting in the Netherlands and Germany, where a voting machine and integrated election software supplied by the manufacturer of the chosen system has been used in real elections.

The report concludes that the introduction of electronic voting in these jurisdictions was relatively uneventful with a focus on the reductions in the numbers of polling stations and election personnel and on the production of earlier and more accurate results. No technical failures occurred to compromise an election count and the only issues arising in public debate were the public availability of the source code, the lack of a VVPAT and the authorisation of the software.

A significant feature of the implementation of electronic voting in the Netherlands and Germany was that the system was tested and certified by a domestic testing agency before being approved by central Government for use locally - such use, in the Netherlands at least, being optional for the local municipality in question.

Although the administrative structures in Ireland are slightly different, there are useful conclusions to be drawn as regards the need to have testing and certification carried out in an Irish context and as regards the desirability of segregation of responsibility as between the procurement function and the type-approval function in respect of the equipment used, both such functions currently being discharged in Ireland by the Department of the Environment, Heritage and Local Government which is also responsible for policy and administration in relation to elections generally.

## **2.9 Other Issues**

### ***Review of Hand-counted Voting System***

A comparison of the performance of the current paper system and the chosen electronic system was carried out for the information of the Commission and the results are reported at *Appendix 2L*.

Eight issues were selected for comparison on the basis that they were considered relevant to the Commission's work. The electronic system was found to be superior on three issues (removal of randomness, prevention of unintentional invalid vote and removal of subjective judgment) and the manual system was also found to be superior on three issues (avoidance of malpractice, opportunity to cast blank vote and transparency and legitimacy).

Of the remaining two issues (relating to major and minor counting errors) it was not possible to say which system was better but it was thought likely that, if the trustworthiness of the electronic system could be established, it would prove superior.

***Rules for the Counting of the Votes***

A recurring issue which arose in various forms in the course of the Commission's work relates to a particular aspect of the rules for the counting of the votes.

Under the current rules, the method of distributing surplus votes involves a degree of variability that could, in theory, affect the outcome of the count in question and/or of subsequent counts. This variability takes two forms.

The first arises when the proportions in which a given surplus is to be distributed have been determined and the next step is to transfer X surplus votes to candidate A, Y votes to candidate B, etc. The question is: Which of the X physical ballot papers should be transferred? The answer is: take X votes from the top of the bundle of papers that have second (or next available preferences) for candidate A<sup>6</sup>.

The second element of variability arises with surpluses that accrue on the second or subsequent counts where, rather than having the whole of an elected candidate's votes examined to establish what proportion of their total votes favours each remaining candidate (and then distributing the surplus accordingly), the proportion of the surplus to be assigned to each remaining candidate is determined on the basis of their share of the continuing preferences in the parcel of votes last received by the candidate whose surplus is being distributed.

Although capable of eliminating this and other minor anomalies in the calculation of proportional distributions of surpluses (i.e. in this case by calculating the proportions in the whole of the elected candidate's votes which would be assigned to each remaining candidate), the chosen electronic system has been designed to reproduce the manual system in exactly its present form.

There is a more accurate method of counting, known as the "Gregory method". This always gives the same result and is in fact the system used in elections to Seanad Éireann. The reason it is not used in other public elections is, presumably, that it is time consuming to implement by hand. However, electronic systems of counting are perfectly suited to handling this method.

The Gregory method of counting could be easily implemented in the electronic system and would increase accuracy of the process and thereby enhance the value of electronic voting by allowing the system to be used to its full capacity. Such a change would, more importantly, be more democratic in that it would allow every relevant preference to be taken into account. Any change to the counting rules would require an amendment to the law governing the various types of elections.

This and some further issues regarding inaccuracies arising from the current counting rules and process are discussed in the report at *Appendix 2L*.

---

<sup>6</sup> The justification for this procedure is that the mixing of the votes at the beginning of the count ensures that the physical papers that are transferred are a random and therefore representative sample of the whole bundle. The problem is that there is a not insignificant degree of variability in the extent to which this is so. To the extent that it is not so, this create potential variability in subsequent counts in which, on an elimination or on a surplus transfer, these transferred ballot papers are examined for preferences for continuing candidates.

### ***Verifiable Audit Trail***

The Commission's terms of reference required it to consider the chosen system, which does not include a verifiable audit trail. However, while the issue of an audit trail therefore does not fall within the Commission's terms of reference for consideration, the Commission sought to establish the feasibility for audit within the system, not least as a useful indicator of "accuracy" as contained in the Commission's terms of reference.

The issues surrounding an audit trail in the context of the chosen system are accordingly set out in a report at *Appendix 2M* which concludes that the chosen system is not feasibly capable of modification to provide a full audit trail without unrealistic cost.

The consequences of this are that while it is possible to independently verify that the votes recorded on ballot modules are those uploaded onto the PC at the count centre, there is no method of validating that the votes stored on ballot modules are those which were originally entered by the voters using the voting machine at the polling centre. The report also outlines a number of alternative voting systems which claim to offer verified voting.

The Commission has noted, in the context of its review of secrecy and accuracy issues, that the existence of an audit trail is principally an indicator rather than a determinant of accuracy and that in certain respects it is inconsistent with the competing requirement of secrecy of the ballot.

### ***Tallying at Elections***

Under electronic voting as currently proposed, the opportunity to "tally" likely results through observation of the ballot papers being counted is lost. A feature of the chosen system which may be used to address, in part, the loss of the tallying function is the facility to publish subsequently the votes cast at an election.

Although this loss of the tallying function enhances the secrecy of the ballot, it also reduces transparency to a level below that which exists in the manual system as regards visual verification of the accuracy of the counting process. Conversely, the proposed remedy for this reduction in transparency, namely, the publication of the votes cast, can have the effect of diminishing voter secrecy in certain circumstances, i.e. where voters deliberately record "signature" voting patterns in lower ranking preferences to make their votes identifiable.

## **2.10 Conclusion**

The work of the Commission as described in this part, together with the public submissions reviewed in *Part 3* are discussed further in *Parts 4* and *5* in the context of the issues of testing, accuracy and secrecy which the Commission is required by its terms of reference to consider.

