Part 3

Public Submissions

3.1 Introduction

By public notices in the newspapers on 11 and 14 March and by radio advertisements in the same period the Commission invited submissions from the public in relation to the secrecy, accuracy and testing of the chosen system. Submissions were to be received by 12 noon on 26 March and interested persons were advised that submissions received would be open to public inspection.

162 submissions were received by post, by e-mail and on line at the Commission's website and a list of the persons from whom submissions were received is set out at *Appendix 3A.*

This part summarises the main points arising from the submissions received and a more detailed summary of the submissions is set out at *Appendix 3B.*

The full texts of the public submissions received are available on the Commission's website *www.cev.ie* and may also be inspected by appointment at the Offices of the Commission during the period of three months following the presentation of this report.

3.2 Persons who made Submissions

The Commission is grateful to the many people, organisations and bodies who made submissions to it and wishes to acknowledge the substantial effort which has obviously gone into the submissions, particularly in view of the short timeframe available. Considerable expertise was made freely available to the Commission in this way and the importance of the public consultation process in the work of the Commission is evident from the high degree of correlation which exists between the main themes in the submissions and the results of the Commission's other work.

The number of public submissions received by the Commission was large, given the short time available. While many submissions were received from ordinary voters, a very large number of submissions came from persons who described themselves as IT professionals. The extent to which these submissions reflect the views of the Irish public as a whole on the proposed electronic voting system is therefore not known.

3.3 Main Themes in Submissions

Most of the submissions confined themselves to matters falling within the Commission's terms of reference, although a significant number argued that the terms of reference are too narrow.

Nearly all of the public submissions were, for various reasons, very hostile to the proposed introduction of the chosen system and to electronic voting in general. Furthermore, some of those few submissions in favour of the proposed system cited an incorrect reason for their support, namely, the elimination under electronic voting of the random element in surplus transfers. In fact, under current proposals, this random element would be maintained.

The following review of the submissions thus necessarily amounts to a classification of the arguments deployed against the proposed system, many of which are overlapping.

The main themes of the submissions received may be summarised as follows:

- the need for a voter verified paper audit trail, to ensure that the accuracy of the results can be checked independently of the new system itself;

- the need to preserve the right to secrecy of a voter casting a blank ballot;

- the need to ensure that the final versions of the hardware and software used in the election are the precise versions that have been tested, approved and certified;

- the need for all software to be open source, to allow the wider community to check that it can generate accurate results; and

- the need for parallel running of the new system with the old paper one, once more to ensure the new system is generating accurate results.

These points concur broadly with the results of the other work carried out by and on behalf of the Commission as set out in *Part 2* and, although the issues of a VVPAT and the blank ballot fall outside the Commission's terms of reference, all have contributed substantially to the Commission's observations, conclusions and recommendations on secrecy, accuracy and testing as developed in *Parts 4* and *5* and as summarised in *Part 6*.

3.4 Summary Review of Submissions

The Need for a Voter Verified Paper Audit Trail

This is overwhelmingly the main argument against the proposed system. In essence the case, repeated many, many times, has three elements:

(a) Reliability

No system is 100 per cent reliable and therefore there will be system failures – if not in the June elections, then at some time in the future. Some of these system failures will be undetectable to those observing the "black box" operation of the system from the outside.

The Irish Computer Society (Submission No. 102), for example, notes that the system has over 200,000 lines of code and, even with the best possible coding practices, past experience implies a minimum of 10 serious system failures during the lifespan of the program. In the event of such a system failure that is detected, the "accurate" election result may be impossible to retrieve without an independent audit trail.

This point is supplemented by arguments that all computer systems in critical situations, such as banking, have an independent audit trail to allow system failures to be retrieved.

This argument can thus be summarised as saying that, sooner or later, there will be system failures, that the accurate result must be independently retrievable for something as important as a public election, and that the proposed system does not have an independent audit trail to allow this retrieval to take place.

(b) Tamper Proof

The view that no system of hardware or software is 100 per cent tamper proof is widespread among both computer professionals and members of the general public. It is reinforced by the view that small electronic ballot modules will be easier for experts to tamper with than large physical ballot boxes, and that ingenious, well-publicised and resourceful hacker and virus attacks show that the technical expertise is available to do this. Examples are given of electronic "back doors" into programs, and viruses that activate at some later date, that will come into effect after "black box" (i.e. non source code) input-output testing is complete.

Such fears are supplemented by a view held by some that security measures controlling access to count PCs and voting machines are not adequate, and that the collusion of staff with technically proficient system attackers would be difficult to prevent.

An independent voter verified audit trail, using random checks involving paper recounts of a limited number of voting machines and count PCs is seen as one way to combat this threat. Again, the proposed system is argued not to have this facility, since the system is seen only to audit itself.

(c) Demonstrable Accuracy

The argument that the election system must, above all, be seen to be accurate is most common among members of the general public. There are many submissions from people who want proof that their vote has been recorded accurately.

The only computer professional mounting a sustained argument against a voter verifiable paper audit trail is William Grogan (Submission No. 92). He argues that this undermines the whole point of electronic voting, would not present a good defence against tampering and is in effect an argument promoted by people who are unwilling to accept that all systems deployed in the real world are inevitably imperfect.

A significant number of computer professionals have argued that the accuracy of the proposed system in a real election cannot be confirmed unless there is some independent voter verified record of voting data with which to compare the computerised count.

The Need for "Parallel Running"

This is a very common argument advanced by the computer professionals who made submissions. Essentially the argument is that, especially for "mission critical" applications such as elections, best practice requires that the changeover to a new system should not be made without running the old system in parallel with it for the first few cycles of the process. This provides an accuracy check by confirming that the old and the new systems generate the same results. This has not happened to any significant extent in Ireland, and certainly not for a national election, with the proposed system. This argument is held to undermine the limited trials of the system for the 2002 Dáil elections and the Nice referendum since there was no parallel paper count to check that both systems produced the same results. A number of computer professionals describe this as "incomprehensible".

Overall, the absence of a voter verified paper audit trail and the absence of parallel running, combined with criticisms of the test regime (see below) make up the vast bulk of both professional and general public objections to the proposed system.

Secrecy of the Ballot

A further class of objections raised in the public submissions concerns potential violations of the secrecy of the ballot. These are somewhat more diverse, although there is widespread agreement on one problem – relating to blank and spoilt votes – and several professional submissions on the secrecy with which votes are stored in the ballot module.

(a) Blank or Spoiled Votes

A submission defending the right of a voter to cast a blank vote, and the consequent right to cast a "none of the above" vote in secret, was made by Karen Devine (Submission No. 116). In this and other submissions, it is argued that voters wishing to spoil their vote or cast a blank or "none-of-the-above" vote must reveal themselves to the voting machine operator. This arises because the "cast vote" button on the voting machine cannot be activated if no preference has been recorded for any election that is taking place on the day. The voting machine operator must then reset the machine immediately after this voter has left the polling booth and will know that the voter concerned has cast a blank vote. In the context of the June elections, this would only happen to voters who refuse to register a preference for any candidate in any election and who also refuse to express a preference in the referendum, but other polls may involve a single election only in which case the casting of a null vote will be impossible[7].

Although implementations of the same system in the Netherlands and Germany allow for the casting of a "null" vote, the particular Irish implementation of the chosen system does seem to force voters who wish to vote for no candidate, and who want to register a blank vote, to reveal himself or herself to the voting machine operator, thus effectively compromising the secrecy of the ballot as far as they are concerned. However, it is understood that the chosen system has been specifically configured for use in an Irish context without this facility on the basis that the Irish electoral code does not formally provide for the recording of null votes. This issue therefore falls outside the terms of reference of the Commission, as does the issue of ballot secrecy being violated for such voters.

Should it be decided to modify the electoral code to provide for the casting of a null vote, even then, while the system could be reconfigured to accommodate this change, it would be unlikely that the reconfiguration could be completed in time for the June elections and it would, in any event, be impossible within this timeframe to carry out the testing that would be necessary to ensure that the modifications had been made without affecting any other aspect of the system.

(b) Random Storage of Votes

It is argued that it may be possible to "unscramble" the order in which votes are randomly stored in the ballot module. The issue that arises here is that, if it is possible to link data on votes cast

[7] The voting machine (as configured for use in Ireland) will not accept a null vote when used at a single poll only. When it is used at multiple polls the machine will allow voters to express preferences in one poll while expressing no preferences in others. However, in the latter case, a vote is only recorded in the poll in which preferences are expressed.

with the order in which people voted on a particular machine, then someone who observed the order of voting would be able to discover precisely how the people observed had voted.

Both the official system documentation and the submission by Powervote Ireland Ltd. (Submission No. 98) describe a system in which votes are stored in random locations on the ballot module. This is challenged in the submission by Irish Citizens for Trustworthy E-voting (ICTE - Submission No. 91) and also in the submission by John Lambe (Submission No. 109) on the ground that what actually happens is that the first record is stored at a random location, the second at a location randomly selected to be one up or one down from that location, and so on. Given knowledge of how the first voter voted, for example, it is argued that it might then be possible to infer how subsequent voters voted.

A related point raised by a number of professionals is the robustness and impenetrability of the pseudo-random number generator used in the program. The point made here is that, since the generator uses a seed taken from the system clock, the random numbers are retrievable by someone who can observe the precise time at which the random number routine was called. This might in some senses seem to be a somewhat arcane and technical problem, however valid theoretically. A risk to security would only arise if there was someone who could accurately record, by physical observation, the order in which voters voted and who had precise information on how some voter voted, and who had access to the addresses at which votes were recorded on the ballot module. It might then be possible to unscramble this order and discover how all voters on that machine had voted. If this claim is accurate, the question that arises is whether the associated risk to the secrecy of the ballot is significant.

(c) Publication of Election Returns

It is argued that it may be possible, on the basis that election returns are published, to bribe or force voters to register a distinctive "signature sequence" in their lower preferences. This point is developed most extensively in submissions by Shane Hogan (Submission No. 100) and William Campbell (Submission No. 157). It relates to the publication subsequent to the count of the complete file of votes cast in a constituency (with voter order randomised) which is part of the current policy.

The claim here is that someone could bribe or intimidate a voter to give a first preference vote in a certain way by requiring that this voter register a distinctive and unique sequence of preferences for lower-ranking candidates. This is in principle feasible, given the huge number of different ways in which an STV ballot can be completed. In the 2002 Dáil election trial in Meath, for example, there were 14 candidates – giving 14x13x12x11x … x1 (= c.87,178,291,200) different ways to complete the ballot. This gives plenty of opportunity for every voter in the constituency to be given a distinctive signature sequence for lower order preferences.

Overall, in relation to ballot secrecy, by far the most common point made in the submissions is that it appears that a voter casting a blank vote may have his or her ballot secrecy violated. In relation to the other points noted above, their significance will be determined by the likelihood that such theoretical possibilities will arise in the real world. This likelihood is dealt with by the risk analysis carried out for the Commission as referred to in *Part 2* and *Appendix 2H*.

System Design, Build and Testing

The universally accepted point that no software or hardware can be guaranteed 100 per cent accurate and effective has already been discussed above. The point made by a number of submissions in this context is that it is necessary to design, build and test any new system as carefully as is feasible, taking account of how "mission-critical" that system is. The more mission-critical the system, the more care must be taken in designing, building and testing it.

A point made in many submissions from IT professionals is that collecting and counting votes in public elections is a highly critical computer application. The implication is that very high standards must be applied to designing, building and testing it – much higher standards than in a less critical home computing application. Some of the submissions cite the extraordinarily high standards applied to the construction and testing of software for NASA space shuttle launches, for automatic pilot computers in airliners, or for major banks. In such critical applications, the significance of secure coding techniques, of comprehensive end-to-end testing, and of all-round "bullet proof" operation of the system in the field, is much greater than at a lower threshold of criticality.

A key issue thus concerns precisely how mission-critical the election count system is. In this context, many of the submissions are critical of the testing regime that has been applied to the proposed system. Criticisms of the design, building and testing of the proposed system can be classified under the following headings:

(a) Overall Design Philosophy

Such criticisms came mainly from IT professionals, none of whom appear to have access to the source code of the system as it has not been publicly released. Indeed the foremost argument is that, as a public resource, the entire source code of the system must be made publicly available, so that it can be subjected to scrutiny and testing by the entire IT community.

The rationale for this is that widespread independent scrutiny of the source code would give much greater public comfort that this code delivers on the objectives of accuracy and secrecy, as well as revealing potential embedded "back doors" and viruses. On this latter point, purists among the IT community have argued that the compiled machine code should also be publicly available, since it is easy for an expert to tamper with a program at machine code level in a way not revealed by the source code. They argue that what is needed is public access to the actual machine code executed on the day of the election by both voting machines and counting PCs.

A complication in making the source code public, alluded to in a number of submissions, is that a large part of the source code is believed to be commented on in Dutch, which many Irish IT professionals do not read.

(b) Software Tools, Design and Architecture

There are submissions from computer professionals (ICTE Submission No. 91, among others) arguing that a weakness in the overall architecture of the software lies in the fact that it is conceived as a single large program rather than as a suite of separate programs. The problem suggested here is that code changes and fixes in one part of the program (e.g. programming the ballot modules) could have unintended consequences elsewhere (e.g. the vote counting routines).

Other criticisms relate to the perceived failure to use much more expensive and time-consuming secure coding systems; the keeping of logs of all code changes; the use of C^{++} as a programming language (claimed to be not as safe for such applications as, for example, Java); the use of Borland Object Pascal; the use of Microsoft Windows as the operating system rather than, for example, an open source platform such as LINUX. These are part of a long list of technical issues raised in the submissions by IT professionals, perhaps the most general of which is the use of the Microsoft Access 97 database, claimed by some to be obsolete, unsupported, insecure (file passwords can easily be cracked using cheap and easily accessible websites) and inappropriate to a large and sensitive application. Reference is made in several submissions to recommendations in independent test reports that the system should be upgraded to the latest version of Microsoft Access, but that a decision was taken not to do this until after the June elections. This latter issue is also addressed in separate correspondence received from Microsoft and discussed further below.

(c) Lack of Comprehensive "End-to-end" testing

A recurring criticism in the submissions from IT professionals was that, while individual component parts of the system have been tested, the system as a whole, with all of its interacting parts, has been inadequately tested, especially in the field at a real election. This relates to the argument about parallel running (see above), since one way of doing end-to-end testing would have been to have run the electronic system in parallel with the old paper system for at least one or two real elections, to check that they generated the same results.

Michael McMahon (Submission No. 160) argues that the twin requirements of accuracy and secrecy in an electronic voting system pose fundamental design problems and that the proposed system in effect sacrifices external checks on accuracy in pursuit of secrecy. He also argues that the collection and aggregation of votes from ballot modules is a part of the system that has not been properly tested, and concludes by recommending, not a VVPAT, but a new e-voting system involving encrypted voter receipts.

(d) Previous Tests

The principal issue raised many times in this context is the claim that much of what has been tested, especially in relation to the software, is not what would actually run in the field in June 2004, given the many updates of the software. Brian Mathews (Submission No. 82) makes the point clearly when he states: "Any tests performed on software are instantly negated once an update is made to that software. The IES software has been through several dozen releases.". He argues that this negates the value of the 2002 general election trials, since "any claims made that the software has already been tested in the last General election are spurious. Whatever software ran then is long gone.". His argument is extended to negate the value of testing in real elections in other countries, since "it is simply ludicrous … to claim that, because one piece of software runs in one country, a totally different piece of software will run in another country". Timothy J. Lane (Submission No. 69) argues that the only safe way to do things is for the final, fully tested and certified, version to be given as a "golden copy" to the electoral authority – this then passes out of the control of the vendor and the electoral authority can be sure that what is running is what has been tested and certified.

Overall, the strong argument is made in a range of submissions that late fixes and upgrades could negate all prior testing, since they could unintentionally introduce new catastrophic problems. It is clearly important in the light of these comments to be certain that the version of

the software that will actually run is the same version that has been subjected to the tests that validated and certified it.

(e) "Black Box" Testing of the Count Routines

Some submissions are unhappy with the approach adopted in the testing of the extent to which the count routines apply Irish electoral laws. Electoral Reform Services Limited (ERS) was commissioned by the Department of the Environment, Heritage and Local Government to carry out "black box" testing as opposed to a code review i.e. to run a series of ERS test cases through both the Powervote Ireland system and an independent system programmed by ERS. This form of parallel testing is known as "black box" testing since it checks that the same input into two independent programs generates the same outputs from both, without looking inside either program.

The criticism made in this context is in effect that there are huge numbers of potential states of the world that cannot be tested, and there is no knowing whether or not one of these might trigger a system failure. The more tests that are run, the better but there may always be some fatal configuration of inputs waiting out there. In fact, while the ERS report in question is criticised for running too few tests, a more recent ERS report of tests carried out in March 2004 indicates that the database of ERS test cases had been increased to around 9,000 sample elections.

3.5 Issues Arising in Other Correspondence

Additional public submissions were received and considered by the Commission after the deadline for such submissions and these to a very large extent make the same points as the submissions already discussed. Some new points were however raised about both the accuracy and secrecy of the system, and some points already made were argued in new ways.

While these late submissions are not being published by the Commission (and are therefore not included in the list of submissions at *Appendix 3A*), those which raised new points are discussed briefly here and are summarised in more detail at *Appendix 3B*.

Secrecy

A submission on ballot secrecy (Submission No. L4) from the National Disability Authority (NDA) argues that the chosen system fails to meet many of the needs of disabled people, despite representations from the NDA following earlier demonstrations of the voting machine. It is argued that many of the problems highlighted affect the secrecy of the ballot for disabled people, since they will need the aid of third parties to vote. Some of these problems exist with the current paper voting system, in which case the argument is that the proposed system is a missed opportunity to improve matters for the disabled, while others, such as in relation to the positioning and layout of the voting machine, are new problems.

These problems are also emphasised by a blind voter and computer expert, Gerry Ellis (Submission No. L16), who not only argues that the ballot secrecy of blind voters is infringed by the proposed system, but that better alterative electronic systems for blind voters are available on the market.

For the most part, it is acknowledged that the proposed system does not seriously lower the secrecy of the ballot for disabled voters, many of whom do not enjoy this under the current paper system, but that it does not take advantage of a good opportunity to improve this.

A further point on ballot secrecy was made by James Doorley (Submission No. L17), a former poll clerk experienced in both paper and e-voting, who argues that the "beeps" made by the machine when registering preferences infringe ballot secrecy in that people outside the polling booth can clearly know how many candidates a person has voted for (a single beep would clearly indicate that the voter had expressed a preference for just one candidate, for example). He also argues that people who do not understand how to use the machine often feel obliged, when asking for help in using the machine, to reveal to the poll clerk how they want to vote.

Accuracy and Testing

Many of the late submissions, as with the other submissions, argued that the accuracy of the proposed system cannot be guaranteed, given the perceived shortcomings in the testing and certification regime. Furthermore, in a submission from Microsoft (Submission No. L5) – defining electronic voting as a "mission-critical" but not "enterprise class" system – significant points about accuracy and testing are also raised in defending the use of the Microsoft Access 97 database system as an integral part of the proposed system.

Microsoft argues that the use of Microsoft Access 97 creates "very little risk to the integrity of the vote" because counting is performed on a "stand-alone, locked down PC". At the same time Microsoft also says that this is not the system it would recommend if the application were being built today. The Microsoft submission, in its defence of retaining Microsoft Access 97 when newer and better alternatives are available, makes the same point stressed by many critics of the proposed system that updated software needs to be completely retested before it can be used in the field:

> "If the application developer, in this case Powervote, makes changes to the code base or underlying platform … then a full detailed verifiable systems test is required".

3.6 Conclusion

Overall, by far the most pervasive points made in the public submissions and other correspondence received were:

- the need for a voter verified paper audit trail, to ensure that the accuracy of the results can be checked independently of the new system itself;
- the need to preserve the right to secrecy of a voter casting a blank ballot;
- the need to ensure that the final versions of the hardware and software used in the election are the precise versions that have been tested, approved and certified;
- the need for all software to be open source, to allow the wider community to check that it can generate accurate results; and

- the need for parallel running of the new system with the old paper one, once more to ensure the new system is generating accurate results.

While the first two of these themes raised in the submissions relate to matters falling outside of the Commission's terms of reference (but which are nonetheless acknowledged in this report as having a bearing on the successful implementation of the chosen system) the Commission has noted that the latter three concur broadly with the main themes of its own work as discussed in *Parts 4* and *5*.

3.7 Inspection of Submissions

The full texts of the public submissions received before the deadline for submissions are available on the Commission's website *www.cev.ie* and may also be inspected by appointment at the Offices of the Commission during the period of three months following the presentation of this report.