Appendix 4

Part 1

Comments of Nedap/Powervote

Comments from Nedap and Powervote
in response to

“Draft Report of the Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System”

version 6.0 18 of June 2004.

And

Public Submissions.

12th August 2004

Mr. A Murphy
Secretary
Commission on Electronic Voting
Kildare House
Kildare Street
Dublin 2
Ireland

Bedford 12th August 2004

Dear Mr. Murphy,

We thank you for your letters of June 30th and July 15th inviting us to comment on the full report containing the Commission's work and on the public submissions received. Although you invited responses from Nedap and Powervote individually we have decided to combine our reply into one document. This is largely due to the fact that there is so much overlap when considering the content of our responses and ultimately what we are discussing is the total Election Management System. The concluding part of this document contains our individual responses to specific items contained in your report.

1 Main points.

The Voting machine (VM), Programming Reading Unit (PRU) and ballot modules with their hardware and embedded software and the Integrated Election Software (IES) when combined together constitute the Election Management System (EMS).

In our 30 years of delivering voting systems to the market it is our experience that the infrequent and somewhat unpredictable nature of elections makes it mandatory to keep the election process as simple as possible. This belief has always been the guiding principle in the development of our voting systems. Furthermore it is our choice to stay as close as possible to the user interface that the voters are used to in paper voting systems; the voting machine has a full face replica of the ballot paper.

We note that the Commissions report states on page 55: "The Commission found the system to be easily understood, both in general concept and in practical use. For election personnel, its operation corresponds logically to the administrative electoral procedures currently in place for manual voting. From the voter's point of view, the "booth" design of the voting machine and the replica ballot interface maintain a useful and helpful linkage to the paper voting procedure. This is not the case with all electronic voting systems".

We also note that the Commission's report confirms that the system can accurately and consistently record and count voters' preferences (part 6 on page 73 points 5, 6, 7 and 8).

The Election Management System (EMS) was designed and delivered in accordance with the specifications and contract s agreed with DOEHLG.

For the Voting machine PRU and Ballot modules these comprise:
- “Requirements for voting machines for use at elections in Ireland DVREC-2” of March 5, 2003.
- “Functional specification – Nedap voting system ESI2 – Powervote version 1.9” of May 5, 2003.

For the IES:
- “Integrated Election Software” in accordance with the Irish Count Requirements and Commentary on the Count Rules dated 23rd June 2000 and administrative procedures defined by DOEHLG.”

All EMS system components were independently tested for compliance on behalf of DOEHLG.
The Voting machine PRU and Ballot modules were tested by the German independent test institute “Physikalisch Technische Bundesanstalt” PTB, including a full source code review of the Voting Machine’s and PRU’s internal software.
The IES was tested by DOEHLG, Nathean in Dublin and Electoral Reform Services in London.
The total system (EMS) was tested by DOEHLG.

Although outside the scope of the terms of reference of the Commission the appendixes 2B, 2F and 2M advocate the use of a voter verifiable audit trail (VVAT). Since this is an issue, especially in the USA, we are happy that the Commission gives this consideration.

We note the fact that the Commission states that a VVAT “ is merely an indicator rather than a determinant of accuracy and in some respects it is inconsistent with the competing requirement of secrecy of the ballot” (page 39) and that “the absence of a VVAT raises the standards and quality of other system testing that is required”. (page 77).
However, in our opinion every voting machine should be designed, built and tested in accordance with the highest standards. Lowering the standards cannot be compensated by any audit trail. Errors or flaws detected during the election would shake voters’ confidence and are unacceptable.

We want to emphasise that a voting machine is used because of the many problems with paper voting. Therefore we cannot rely on VVAT with manual paper counting to check voting machines. In this respect we refer to the report of Michael Ian Shamos that was published April 2004
(www.cpsr.org/conferences/cfp93/shamos.html).

In our opinion a VVAT adds problems instead of solving them and makes the election process more complex and does not increase voters trust. This issue was also addressed by Ted Selker and Jon Goler both from MIT in their Voting Technology Project working paper of April 2004.
(www.vote.caltech.edu/Reports/vtp_wp13.pdf).

It is our belief that testing by an independent test institute gives the voters the confidence that the system accurately and consistently records, stores and counts their votes. In case of any doubt, parallel testing before or on Election Day could enhance voters confidence.

It seems to us that the different backgrounds of the testers and evaluators have lead at times to findings with a focus on each of their fields of experience and that thereby they did not take into account the nature

of the very specific election processes which the chosen system has been designed to deal with. In any risk analysis it should always be a question of: "what risks are tolerable and acceptable".
The field of experience of the investigators is clearly visible in their respective reports.

The appendix 2G "Assessment of Documentation and Procedures" investigates the controls of the proposed system. Knowledge of control arrangements is shown here.
The conclusions are:
"The overall control environment, within the electronic voting system, is quite strong" (page 248) and "In summary, the system is a modern and innovative enhancement that can, in our assessment, command confidence. It will be secure if the guidelines and procedures are complied with. It is more transparent, in several aspects than the older manual system used heretofore." (page 265).

The appendix 2C " Evaluation of Voting Machine, Peripherals and Software" reports a test with a representative sample of more than 10% of all voting machines with an in depth analysis of the results, and reports further the reviews of previous tests and a risk analysis. The coverage of the investigations is very broad. One can assume that the investigators have experience with voting systems.
The conclusion is: (a) that the voting machines deployed for use in the June 2004 European and Local elections are a reliable means of recording the votes of the people and (b) that, provided that our critical requirements are implemented and that the aspects of the system we have not examined are shown to be satisfactory, the chosen electronic voting system can be safely used in the June 2004 elections (page 191).

In appendix 2H " Risk Analysis" risks are identified and judged for their acceptability. Experience with risk analysis is evident here.
The conclusion is: 49 risks are identified, 5 of them being material risks which can be addressed by proper procedures and testing (page 273).

The appendix 2B "Review of hardware, Software Security and Testing" advocates the use of cryptography to deal with a number of risks and raises questions about the randomisation, without considering the acceptability of these risks. Here the focus on IT is clear.
The conclusion in appendix 2B is: "we would have serious concerns about the integrity of any election carried out using the current system" (page 130).

As indicated above, the findings that are reflected in the appendices are sometimes contradictory.
From reading the recommendations we conclude that the Commission has recognised this.
However, if the reports are published, they could lead to misunderstanding when read by a superficial reader.

In appendix 2B the conclusion is drawn (page 129, page 138) that the Nedap voting machine uses old-fashioned technology. The main reason for this statement is, as appears from the report, that cryptography is not used and the randomisation is questioned.

This would imply that by use of other technology the system would be a better one.
It is our view that secure key-management that is associated with cryptography adds to complexity of the election process where the risks can be neutralised by procedures, while the risk induced by the chosen randomisation is low and only exists in the first minutes of operation of the voting machine. This is explained in more detail in the Nedap section of this response.

It is the balance in concept, ease of use, proven technology, procedures and workload that makes the chosen system optimally suited for use at elections in Ireland.

2 Recommendations.

Where the commission makes their recommendations for action on page 78 we comment as follows:

- **There needs to be a final definitive version of the software and all related hardware and software components to be used at elections in Ireland.**

  The hardware and software of the voting machine are the final definitive version, as tested by the PTB.

  Any IES software to be used would be tested prior to its general use by DOEHLG and other bodies they may appoint. Due to the infrequent and unpredictable nature of statutory polls it is essential that any requested changes to IES can be implemented and tested within agreed timescales. Appropriate testing of the definitive version was planned to allow sufficient time prior to the polls in June 2004.

- **There then needs to be a full independent review of the source code and testing of the final system to be used: any subsequent software modification would require a further full system retest.**

  Individuals are not independent whereas Independent Test Authorities with formal accreditation are. Our recommendation would be to appoint ITA's for the sake of independence when examining the source code.

- **There should be independent parallel testing of the system, including where possible in live electoral context.**

  We encourage the conduct of parallel testing if it can enhance voters trust. This parallel testing should be done with the real poll(s) data on randomly selected voting machines on or before the Election Day.

- **There should be independent end-to-end testing of the system.**

We encourage the conduct of independent end-to-end testing of the system as it can enhance voters trust.

- **There should be testing and certification by a single accredited body of the suitability of each new version of the entire system for use at elections in Ireland.**

From a detailed review and discussion with a single accredited body it can be determined which are the precise range of tests which need to be carried out in order to certify the suitability of each new version of the entire system, taking into account the nature of the change that leads to a new version. We therefore welcome the Commission's expressed preference to choose an accredited body.

The DOEHLG contracted us to supply an electronic voting system. Although this is described in terms of hardware and software it has also included contributions drawn from our successful, collective experience spanning 30 years and covering many subtleties associated with the practicalities in the application of technology to the democratic process. This experience is available to the Commission and we look forward to assisting where appropriate.

Remaining pages of this document contain specific comments from Powervote and Nedap individually in response to the documents provided by the Commission.

Yours Sincerely

Roy Loudon
Powervote Ireland Limited

Henk Steentjes
Nedap NV

NEDAP (Voting Machine, PRU and ballot module)

The following comments are offered following a first review of the documents provided. We have focussed on specific items. Should the Commission require clarification of any item not dealt with in our response we shall be pleased to assist. We reserve the right to amend or add material should it become available.

Appendix 2A Evaluation of the previous testing Part 1.

Issue 3: The IES and PRU cannot be checked for authenticity, so no testing has been carried out for this issue. (page 97).

The PRU can be checked for authenticity. Commands for ID, hardware version and software version are available.

Issue 5: Download of election information from IES to ballot module can be checked using manual procedures. It has not been verified that there is no possibility to transfer 'extra' data from IES to ESI2 via the ballot module. (page 98).

This is implicitly tested by the code inspection carried out by the PTB. The fact that interference between program modules is not allowed (nichterlaubte Rückwirkungen) is always tested.

Issue15: The test documentation does not, however, explain what happens if power fails while a vote is being stored in the ballot module, e.g. 2 of the 4 write operations have been completed, and the 3rd is underway. It needs to be clarified whether this is possible, and whether it might corrupt the modules vote memory. (page 103).

If the power failure occurs before the pressing of the cast vote button the vote is not stored. If the power failure occurs after the pressing of the cast vote button the votes are stored in fast memory and are stored in the ballot module after the return of power, the number of votes is increased. If the vote is not stored successfully after the return of power then an error message is displayed. This has been tested by the PTB.

Issue18: It has not been tested that the backup is an exact copy of the primary ballot module. (page 104).

Although not an explicit test, it is implicitly tested by code analysis and code inspection by the PTB.

Issue 21: The relevant IES software has been desk-reviewed by Nathean. However, the PRU's role in the reading procedure has not been independently tested or desk reviewed.

The software of the PRU is part of the software package for the voting machine that is tested by the PTB. The communication is tested. Only defined items are transferred. The reading of votes is implicitly tested by code analysis and code inspection by the PTB.

Appendix 2B Review of hardware, software, security and testing.

1.1 executive summary of findings
Security Policies & Software assurance
1. There is no well-defined comprehensive security policy covering the development, deployment or use of the system. (page 129).

Development of the VM is done under ISO 9001 and includes controlled access to development environment. We developed the voting machine and PRU in accordance with the specifications of DOEHLG:

- "Requirements for voting machines for use at elections in Ireland DVREC-2" of March 5, 2003.
- "Functional specification – Nedap voting system ESI2 – Powervote version 1.9" of May 5, 2003.

For deployment and use we always work together with our customers to determine which procedures are to be put in place. Wherever possible and desirable we try to stay close to the procedures that are used in paper and pencil based voting.

2. A number of important security goals have been specified and a significant amount of effort has been expended to ensure that these goals have/will be met. However, the equally important goals of voters' trust in the system and prevention/detection of insider attacks have not been fully addressed. (page 129).

In our opinion voters trust can be gained by the judgement of an accredited test institute. An important element is the definition of the test criteria. If necessary, voters trust could be enhanced by parallel testing before or on Election Day. Prevention and detection of insider attacks can be secured by procedural measures.

Hardware / software interface
1. Nedap voting system is 1980 technology. In the 1980's the threats to this kind of technology were not as well understood as they are today; furthermore many effective defence counter-measures have been perfected in the meantime (such as the use of Cryptography) which are not deployed here. (page 129).

This would imply that by use of other technology the system would be a better one. It is the balance in concept, ease of use, proven technology, procedures and workload that makes the chosen system optimally suited for use at elections in Ireland.
Encryption has not been used for several reasons.

- The key-management of encryption makes the process more complex. Elections are never a routine because of their occasional and at times unpredictable nature. Therefore our goal is: <u>keep it simple!</u>

- The vulnerability of attacks can be secured by procedural measures without adding complexity to the process. See the next point.

2. Security is inadequate. A determined individual insider with short-term access to a voting machine, ballot modules or the count-centre computer could significantly affect the recorded votes. With the possible exception of the voting machine such tampering could be done in an undetectable fashion. (page 129).

Although it is an implausible scenario for the voting machine software, this risk can be considerably reduced if not eliminated by appropriate procedures (Appendix 2H risk 6.1). The ballot modules can be transported from the polling station to the count centre in a sealed container. (Appendix 2H risk 6.4 page 302/303), or could be transported by at least 2 people. Attacks on the voting machine and ballot module can be detected by parallel testing (Appendix C page 155, bullet 6).

3. Security, such as it is, relies largely on the long discredited concept of "Security Through Obscurity". It is a well-established principle in the world of electronic and computer security, that this is inadequate. (page 129).

Revealing every aspect of the design would give greater knowledge to those who may wish to tamper. So obscurity has a value. Proper procedures must be part of the plan to inhibit people from tampering. Security is always based on a combination of procedures, technology and obscurity. Also cryptology relies on this combination: the key to encrypt or to authenticate data must be kept secret, usually by a small group of people.

2 Security Policies and Software assurance.

2.1.3.a In general, only the external operations of the systems appear to be audited. For example, users are required to complete paper documents and attach printouts from the VM and IES software. There does not appear any audit information generated and stored automatically as the system is being used. (page 131).

In addition to the information in the Open Poll Statement, Close Poll Statement and information on authenticity of hardware and software, settings, election information like number of votes cast, the voting machine logs the status changes and the errors combined with a timestamp. This information is available in the special "service mode" and intended for 1st echelon analysis.
It appears that this audit log meets the " draft recommendations of voting standards for e-voting" currently under development by the Council of Europe.

2.2.3 It is generally accepted that obtaining assurance after software has been developed is problematic and the recommended approach is to use an assured development methodology

throughout the lifecycle of a software product. There is no indication that such a methodology has been used during the development of the NEDAP/Powervote system. (page 133).

The software development methodology used for the voting machine conforms to ISO/IEC 12207 and includes the phases of

- specification
- software design
- coding
- testing (module and integration testing)
- and in parallel of the above: documentation, change management control and test case design.

2.1.3.e Voters trust could be established by the participation of a Trusted Third Party in the operation of the system or better still, the use of a Voter-Verified Audit Trail (VVAT). (page 132)
2.3 Transparency & Trust. (page 133)

Voters trust can be established by:

- The judgement of an independent accredited test institute, and if necessary
- Parallel testing on or before Election Day.

This judgement, if necessary combined with parallel testing, gives the voters the confidence that the system accurately and consistently records, stores and counts their votes.
The Voter Verified Paper Audit trail, a printer that prints a paper copy of the vote to be verified by the voter does not bring confidence to the voter but on the contrary, can take away voters trust. The best way to insure the correctness of the VM's software for that particular election is parallel testing before or on Election Day.
In the report of April 2004 "security vulnerabilities and problems with VVPT" written by Ted Selker and John Golen both from MIT, it is stated that the difficulties in the areas of ergonomics, logistics, security, fraud and mechanical stability are of a nature that voter verifiable paper trail (VVPT or VVPAT) cannot be the answer to increase voters trust and above all it infringes the principle of "make it more simple, not more complex".

A1. Randomisation (voting machine). (page 144)
Resume: It is possible to reveal the votes by using a microphone to pick up the beep of cast votes button. When the first vote is known than the rest of the votes can be determined.

Due to the inaccuracy of the system clock, 2.7 minutes (8msec/50ppm) after start-up of the voting machine one cannot be sure any more what the precise counters value is. The probability and the impact of the risk are both very low.

Appendix 2C Evaluation of Voting Machine, Peripherals and Software.

Executive summary.
The control unit (which controls the selection of the races available to each voter and determines

the disposition of incomplete ballots [those that have not been confirmed by a second push on the cast vote button]) requires continuous oversight by at least one other person. (page 156)

The operation of the control unit is dealt with in detail during training of polling station staff. Instructions are also included in the Voting Machine Operators Guide.
Voter education includes specific emphasis on pressing the cast vote(s) button prior to leaving the machine.
Should a voter leave the voting machine without completing the voting cycle completely then the member of staff at the control unit will be aware of this. They can then take the appropriate action as specified by the Returning Officer.
We do not therefore see the need for an extra member of staff to be present at the control unit.

5 Input –Output test of voting machines.

We take notice that 739 voting machines have been tested with 1 national constituency with 12 candidates and 36,950 simulated ballots (50 ballots per voting machine). Also a parallel videotaped experiment was conducted with 5,000 votes. (page 167-179).

The conclusion is:
In balance however, we conclude that the voting machines deployed for use in the June 2004 European and Local elections appear to be a reliable means of recording the votes cast by the voters. (page 179).

11.1 Critical requirements
All software portions of the system should be authenticated. It is worthwhile noting that very little of the voting process is secret – the contents and order of the ballot papers, and the details of the votes (once they are not identifiable with the individual voter) are all public knowledge. The only requirement is that they be accurate. The only secret is the specific vote cast by a specific voter. Hence authentication of data is essential, but not encryption. (page 190).

To determine that the voting machines and PRU’s embedded software has not been tampered with, parallel testing is the best method. Attacks on the voting machine and ballot module would be detected by parallel testing (Appendix C page 155, bullet 6).

12 Conclusion.
Overall, however, we conclude (a) that the voting machines deployed for use in the June 2004 European and Local elections are a reliable means of recording the votes of the people and (b) that, provided that our critical requirements are implemented and that the aspects of the system we have not examined are shown to be satisfactory, the chosen electronic voting system can be safely used in the June 2004 elections (page 191).

Appendix 2G Assessment of Documentation and procedures.

Summary conclusion.

We note:
The overall control environment, within the electronic voting system, is quite strong. Indeed, in some respects, the electronic system is likely to produce greater accuracy and avoidance of potential human error. It will also lead to significantly enhanced efficiency at the count. (page 248).

8.0 Main findings and Recommendations.

We note:
In summary, the system is a modern and innovative enhancement that can, in our assessment, command confidence. It will be secure if the guidelines and procedures are complied with. It is more transparent, in several aspects, than the older manual system used heretofore. However, it requires more advanced planning and testing initiatives than previous systems. It can be successfully administered; assuming the right election staff can be recruited, appropriately trained and deployed at polling stations and at other levels. (page 265).

Appendix 2H Risk Analysis.

Summary of conclusions.
The latter three risks can be considerably reduced, if not eliminated, by appropriate procedures. The first two risks cannot be dealt with this side of the June 2004 elections. (page 273).

The Voting machine PRU and Ballot modules were tested by a number of test institutes including the German independent test institute “Physikalisch Technische Bundesanstalt” PTB that conducted a full source code review of the Voting Machine’s and PRU’s internal software.

Finally it should be noted that many of the risks identified below only exist because of the absence of an independent verification mechanism for the results such as an audit trail. (page 273).

An audit trail could only show that the event, identified as a risk occurs on Election Day, but that is too late!! In our opinion every voting machine should be designed, built and tested in accordance to the highest standards. Lowering the standards cannot be compensated by any audit trail. Errors or flaws detected during the election would shake voter’s confidence and are unacceptable.

Appendix 2I Secrecy of the ballot.

Summary of conclusions.
There is a material threat to the secrecy of the vote when a voter abstains, i.e. does not press the

'cast vote' button. This could be easily eliminated by putting an abstain button on the machine. (page 309).

During the preparation of the specification for the ESI-2 voting machine DOEHLG decided not to include an abstain button facility. The ESI-2 voting machine can be modified to include an abstain button.

Appendix 2L Comparison of Electronic Voting and Paper Voting in Ireland.

For a comparison between paper voting and electronic voting we would refer the Commission to the report of Michael Ian Shamos that was published April 2004. (www.cpsr.org/conferences/cfp93/shamos.html).

Appendix 2M Feasibility of audit.

We want to emphasise that a voting machine is used because of the many problems with paper voting. Therefore we cannot rely on VVAT with manual paper counting to check voting machines.
It is our belief that a VVAT adds problems instead of solving them and makes the election process more complex and does not increase voters trust.
This issue was also addressed by Ted Selker and Jon Goler both from MIT in their Voting Technology Project working paper of April 2004. (www.vote.caltech.edu/Reports/vtp_wp13.pdf).
It is our belief that testing by an independent test institute in combination with parallel testing on or before election day gives the voters the confidence that the system accurately and consistently records, stores and counts their votes.

Appendix 3 Public Submissions.

A very large number of the submissions (approximately 80%) were from people who describe themselves as IT professionals.
It seems to us that they focussed on specific IT solutions and did not analyse the acceptability of the risks involved or considered other options that are available without making the election process more complex.

POWERVOTE (Integrated Election Software)

The following comments are offered following a first review of the documents provided. We have focussed on specific items. Should the Commission require clarification of any item not dealt with in our response we shall be pleased to assist. We reserve the right to amend or add material should it become available.

Page **comment.**

29 **Software Evaluation**

(a) Review of previous tests.

In the original tender document (section - Count Requirements and Commentary on Count Rules dated 23rd June 2000) there was an explanation of the calculation used in the count rules (section 7 – point 3.2). The presentation was described in section 19 and also explained how the remainders should be presented. IES was designed to comply with these documents.

As part of the testing programme initiated by DOEHLG the company ERS was instructed to test IES under a number of unusual and extreme STV election samples they hold. It was felt that these types of examples were unlikely to be encountered in practice but at the same time were viewed as a good vehicle to exercise IES fully. These tests were conducted late February early March 2004.

ERSs conclusion was that under some of their particular rare test cases IES may not produce the correct result. The solution was to increase the number of decimal places available within the remainders. From advice given to DOEHLG by appointed testers the Department determined that IES should be modified to eliminate even the rare possibility that such situations maybe encountered in practical polls in Ireland.

IES version 129 produced in March 2004 included a minor change to deal with this.

ERS carried out tests on version 129 (8,776 test cases) and produced a report to DOEHLG. This report indicated that the IES count section was a correct interpretation of the Irish Count Requirements and Commentary on Count Rules .

(b) Further Tests Carried Out.

The findings of the Coyle-Doyle Implementation are acknowledged. It is caused by a rounding problem and subsequent issues of IES will be adjusted and tested accordingly.

31 **(e) Review of source code.**

It was not possible for the Commission to obtain access to the full source code of the system. This was due to the fact that the Commission at the time of request was not a legal body and could not give any specific undertakings. In an effort to assist the Commission as much as possible whilst maintaining commercial prudence we decided to release the count section of IES for code review.
Further release of source code for review will be covered by non-disclosure agreement.

48 **(a) Overall Design Philosophy**

Assuming that a system has been fully tested to agreed parameters by an ITA then why does it need to be made publicly available? Perhaps a more appropriate consideration would be to make a section available. In the case of the system perhaps it could be the count section only where interested parties could check.

48 **(b) Software Tools, Design and architecture.**
The programme contains 2 executables, IES and PRVOTES.
IES contains all administrative and count units, PRVOTES is the connection to the Programme/Reading Unit (PRU).
A suitable test regime would enable comparator tests to be conducted between a known standard and any new issue.
All testing undertaken or sponsored by DOEHLG has not found issue with the overall design philosophy of IES.
IES can operate with the latest version of Microsoft Access. Collectively, DOEHLG, Nathean and Powervote chose Microsoft Access 97 as it is tried, tested and proven. Microsoft confirms that it is adequate for the chosen standalone application of IES.

(d) Previous tests.

As previously mentioned we support comprehensive testing. The test regime employed must take account of the infrequent and at times unpredictable nature of statutory polls, and the lead in time. Any version of IES to be used would be the same version that has been subjected to the tests, which validated and certified it.

51 **Accuracy and testing.**

As mentioned in (b) above IES can be adapted to other databases should that be deemed to be required.

55 **Previous Use of System.**

We are pleased that your investigation of the use of the system at the Dail and Nice referendum of 2002 showed that votes recorded had been counted correctly.

58 **Scope and Context of Tests. Paragraph 4.**

DOEHLG instructed Nathean to test IES.
Some extracts from their reports are listed for reference;

1st review, 14-12-2001
In general the source code has been well written and with a few exceptions seems to implement the count rules correctly.

Review build 0111, 3-10-2003
Overall, the review gives the coding standards a clean bill of health. All previous recommended coding standards have been observed.

Review build 0124, 26-03-2004 and build 132, 20-04-2004
The source code demonstrated adherence to the best practice requirements set out by previous reviews.

58 **Relevance of tests.**

See our comments under page 423, 6.2.

60 **Range of Tests.**

We are very pleased that the tests sponsored by the Commission proved that the system functioned according to the agreed specifications.
The error mentioned regarding the calculation of fractions was rectified and tested in version 129 of IES. Independent test results were accepted by DOEHLG.
We note that the Commission seek more testing of the system. Assuming that these tests are discussed, agreed and carried out by an independent accredited body then we will provide the necessary assistance and co-operation.

65 **5.2 Accuracy.**

In the context of collecting and counting the votes there are
inherent imperfections when using the pencil and paper system.

Benefits.

IES could be re-designed to implement the Gregory method. As stated in the report this would require an amendment to the statutory rules for the counting of votes.

Issues of Concern.

(a) the final version of the software would have been delivered within timescales agreed with DOEHLG to allow for final testing and verification.
(b) The error reported by the Commission was rectified from version 129 onwards.
(c) The possibility of inadvertent voter error is reduced through the use of the chosen system.
(d) As already stated IES can be re-designed to remove the mixing element at the count.

73 **Summary and conclusions.**

6.1 General Observations

We are pleased that the range of tests on the chosen system produced overall favourable conclusions.

6.2 Testing, Accuracy and Secrecy

The nature of statutory elections and referenda mean that any software system used for the administration and conduct of these must have in built flexibility to be able to implement changes very quickly.
When we began developing the IES version for Ireland it was agreed with DOEHLG that the first priority was to start with the count section. Following the completion and testing of this then work began on the electoral administration section of IES.
Changes to the count rules are unlikely whereas administrative procedures are in our experience subject to more frequent changes. The changes to IES resulting in new versions being issued and noted by the Commission, are due to text and presentational requests from DOEHLG. The numbers of requests were greater than normal as IES was being prepared for nation-wide introduction. Unlike the previous pilots the June polls were to use multiple ballots and a different count and reporting structure in terms of constituencies, local electoral areas etc.
We remain satisfied that time would have permitted testing of the version to be used at the June polls by the methods agreed with DOEHLG.

108 **Issue 25.**

It seems to be suggested that we made 2 versions of IES. One for ERS to conduct their tests and another for DOEHLG. We neither sought nor were given any such permission.

132 **2.2 Software Assurance.**

See our page 31 response.

135 **3.2 Examination of Nathean Code Review**

The statement which is discussed regarding the pseudo code is only in the report and NOT in the source code of IES.

137 **3.6 Ability to produce printed ballot papers.**
This facility is described in the electoral act and was included in the tender document.

155/156 **Appendix 2C Evaluation of Voting Machine, Peripherals and Software. para5.**

This section contains qualitative and quantitative material. Whilst we are not in complete agreement with all of the recommendations we are pleased that the 'mock poll' testing involving 739 voting machines was satisfactory.
Some of the points raised will be discussed with DOEHLG.

179 **6. Using IES from the Local Electoral Area/Constituency Worker's Perspective.**

A CD is generated with ballot details. It is important to note that a hard copy of the contents of the CD (printed ballot)is also sent with the CD. This is to enable the recipient to verify the data contained on the CD.

Where appropriate the other points raised will be discussed with DOEHLG.

182 **6.2 There should be some way of ensuring that the correct picture is associated with the correct candidate.**

Candidates are obliged to submit a printed, verified copy of their photograph with the CD image. This would occur at the point they register as a candidate with the Returning Officer for each poll.

207 **5 Miscellaneous software and usability issues.**
Paragraph 2.
Failures regarding the export of screens.

This was known about for sometime. The function worked according to the specification on our PCs. We were unable to replicate the problem encountered by DOEHLG on our PCs.
When we received a sample of a specific election PC from Ireland we were able to identify the problem. A small difference between Word 2000 Ireland vs Netherlands edition was the cause. From version 134 of IES this was rectified. It was tested by DOEHLG and found to be functioning correctly.

231 **Use of an updated version of the IES software.**

The LGCSB issue IES to each user. At the time that the user loads IES onto their system they must send confirmation from IES of this to a central location. By using this method it is then known that all users have the same version installed and operating.

Any testing previously carried out on the software may no longer be valid as a result of changes made to the software.

The testing regime would ensure validity of software is maintained.

320 **Experience of Electronic Voting Overseas**
4.4 United Kingdom

The report starts from 2002. We wish to point out that the Powervote system was the first ever Home Office approved UK authority wide pilot of electronic voting and counting in May 2000. Stratford on Avon District Council was the piloting authority. The pilot was very successful. This lead to further pilots in 2002 and 2003.
Powervote has an agreement with the UK government which extends to 2006 as part of their on going piloting.

324 **Appendix One. Table of comparative experience with electronic voting systems.**

The entry for the UK is inaccurate in that it only mentions Sequoia Voting Systems. See our comments relating to page 320 above. To our knowledge the first authority wide UK pilot involving Sequoia was in 2002.