Appendix 7A

Comments of Nedap

Nedap Comments[83] on Summary Conclusion, Executive Summary and Recommendations

Mr. Alan Murphy Secretary
Commission on Electronic Voting
Floor 4
Setanta Centre
Nassau Street
Dublin 2
Ireland

9th June 2006

Dear Mr. Murphy,

In your letter of May 17th 2006 and in your letter of June 2nd 2006 you invited us to comment on the final draft (version 6 and selected pages of version 6.2) of the second report of the Commission concerning the secrecy, accuracy and testing of the chosen electronic voting system.

When reading version 6 and the amendments in version 6.2 of the second report we noticed that on a number of issues the Commission has taken into account our comments we made previously on your invitations.

For completeness we list these documents:

- Our letter and enclosure of April 11th 2006 with our comments on version 3.9 of Part 1 (Introduction), Part 2 (Work of the Commission) and Part 7 (Summary, Conclusion and Recommendations).
- Our letter and enclosure of February 14th 2006 with our comments on version 3 of Part 3 (Technical Aspects and Testing of the Chosen System).
- Our Letter of March 2nd 2006 with our comments on version 3 of Part 4 (Physical and Operational Security Aspects of the Chosen System.
- Our letter and enclosures of March 20th 2006 with our comments on version 3 of Part 5 (Comparative Assessment of the Chosen System and the Paper System).
- Our letter and enclosure of March 9th 2006 with our comments on version 3 of Part 6 (e-Voting Best Practice: Council of Europe Recommendation).

However we do not see the essence of our comments incorporated in version 6. These are:

- The VM, PRU, BM and embedded software have been adequately evaluated and tested by accredited Independent Test Authorities according the specifications agreed with DOEHLG in 2003.
- In terms of secrecy, accuracy and other important criteria the qualities of the VM, PRU, BM and the embedded software outweigh the current paper system.

[83] At the request of Nedap, these comments have been reproduced by the Commission in the form they were received, subject only to the deletion of page references as they relate to earlier drafts of the Commission's report. The comments also refer to text contained in earlier drafts that has been revised in the final version of the report.

For that reason we leave the comments that we gave on parts 1 to 7 of the second report unchanged.
Accordingly we restrict the following comments to the summary conclusion, the executive summary and the parts 8 and 9 of version 6 and the amendments in version 6.2.

We request that you publish these comments and our comments and enclosures on versions 3 and 3.9 of the Parts 1 to 7 as mentioned on page 1 of this letter in full as part of the report, with the exclusion of the enclosure of part 7, since its items are commented in the parts 8 and 9.

As you know our comments relate to the Voting Machine (VM), the Programming Reading Unit (PRU) and Ballot modules (BM) with their hardware and embedded software.

1. Summary Conclusion

a) Voting and Counting Equipment.

We note the positive findings of the Commission regarding design, hardware components and software of the VM and relating hardware components:

The voting machine and related hardware components are of good quality and their design, which is based on voting systems that have been reliable in use elsewhere for some years, has also remained stable since their adaptation for use in Ireland.

We comment on the following conclusions

- *Subject to some minor security and usability enhancements, followed by extended and rigorous testing once it has been so modified, the voting machine can be confidently recommended for use.*

- *The software of the voting machine is also of adequate quality, requiring only minor modifications followed by further analysis to confirm its reliability.*

The VM, PRU, BM and the embedded software have been delivered according the specifications agreed with the Department. Any modifications in the hardware or software can only be made after these modifications have been incorporated in the specifications.

We comment on the following conclusion

- *Improvements are also required to the security of the methods by which sensitive election data, including votes, are stored, transported and accessed on ballot modules and CD's.*

Since the risk of attempted access is eliminated by the required procedures that prevent accidental or deliberate loss or damage there is no need for encryption (to maintain the confidentiality of the data) and there is no need for cryptographic signing (to protect against any attempted alteration) as recommended in R.10 of part 8.

b) Security Management.

The Commission has also recommended improved physical and operational security measures that do not require

modification of the chosen system but that can significantly enhance its overall security.

The evaluation and testing of the hardware and software demonstrate the quality of the hardware and software of the VM, PRU, BM and the embedded software and show that no failures have been detected. In our opinion it is important that attention is focussed on the procedural side of the election process, including the physical security.

c) Comparison with Paper Voting.

Following the comparative assessment against the paper system of voting that it was requested to carry out, the Commission has concluded that, in terms of secrecy and accuracy, the paper system is superior to the chosen system as currently proposed but that, subject to the Commission's recommendations, the chosen system has the potential to deliver greater accuracy that the paper system and can provide similarly high levels of secrecy.

We are convinced that in the current situation the chosen system is superior to the paper system (see our comments on part 5 in our letter and enclosures of March 20th 2006).

We recommend the use of the chosen system as currently proposed in a small number of constituencies as soon as possible. It would present a strong signal to the Irish voters and the proposed procedures could be fine tuned.

2. Executive Summary

a) Key Findings and Conclusions

- *Hardware and software*
- *System and Data Security*
- *Testing and Independent Verification*

We note the positive findings of the Commission on the Hardware and software of the VM, PRU and BM.
As we have shown in our comments on part 3 of the second report in our letter and enclosure of February 14th 2006 the requirements, standards and test criteria that were applicable for the design, evaluation and testing of the VM, PRU, BM and the embedded software are adequate with respect to electronic voting practices in Europe, which were developed over the last decades and we have shown that the evaluation and testing done by the ITA's have proven satisfactorily that these components of the chosen system provide the necessarily secrecy and accuracy.

- *Physical security*

We show in our comments on part 4 of the second report in our letter March 2nd 2006, that further work should address the procedural side of the election process.

- *Comparative Assessment against Paper Voting*

We show in our letter and enclosures of March 20th 2006, containing our comments part 5 of the second report, that the VM, PRU, BM and the embedded software outweigh the paper system in terms of accuracy, secrecy and the other important criteria mentioned in version 3 of part 5 of the Commission's second report.

b) Overall Conclusion

We note some highlights from the Commissions overall conclusion.

- *Based on the results of its work to date in relation to technical, procedural and comparative aspects of the chosen system, and recognising that the chosen system can potentially enhance and deliver real efficiencies in the administration of elections, the Commission concludes that it can recommend the voting and counting equipment for use at elections in Ireland, subject to further work it has also recommended …*
- *Further development, testing and analysis of the system, followed by independent certification of its suitability are thus necessary before it can be confidently be used at elections in Ireland.*
- *Approaches to further development, testing and analysis of the system have also been recommended with a view to providing the necessary assurances that the system is reliable.*
- *Subject to this work being carried out in accordance with the recommendations of the Commission, it is likely that the chosen system can be deployed and used with confidence in the future.*

It is remarkable that in the eyes of the Commission the official tests and validation undertaken to date are insufficient to provide the requisite levels of confidence, although the VM, PRU, BM and its embedded software system were independently reviewed and tested on behalf of the Department by ITA's for compliance with the requirements of 2003 that were issued by the Department of the Environment, Heritage and Local Government.

c) Electronic voting context

We note the positive view of the Commission, where it recognises that, when compared with paper voting, electronic voting methods in general can deliver enhanced levels of accuracy and similar levels of secrecy and that this potential also exists in the particular case of the chosen system.

3. Part 8 of the second report

Recommendations

The Commission recommends that the following steps are necessary, as a minimum, to ensure and confirm the secrecy and accuracy of the chosen system before it could confidently be used at elections in Ireland.

On a number of important issues we have a different opinion than the Commission. In our comments to the Commission on the second report we have proposed alternatives where applicable. Eventually it will be up to the Irish Government to decide how to proceed with electronic voting in Ireland. We will consider any future proposals of our customer, the Department of the Environment, Heritage and Local Government with a positive attitude.

We comment on the Commissions recommendations where applicable for the VM, PRU, BM and the embedded software.

Hardware, Software and Peripherals

R.1: *Protections against potential vulnerabilities or weaknesses of the voting machine, programming/reading unit and ballot module identified by the Commission (section 3.2) should be placed beyond doubt by further independent analysis and testing of the embedded C code software that governs their functions.*

In our opinion the embedded software of the VM, PRU and BM is adequately analysed and tested by the accredited German Independent Test Authority "Physikalisch Technische Bundesanstalt" (PTB) against the test criteria derived from

- "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

This analysis included a manual source code inspection that discharged potential run-time errors.

R.5: *Measures should be introduced to allow the authenticity of the hardware and software components of the system to be independently verified by operators and observers.*

The following two aspects guarantee the reliability of the hardware and software.

- The source code of the software is only available to Nedap and the ITA's.
- The Voting Machine is stand-alone and its software or hardware cannot be accessed from the outside and this also applies to the PRU.

The authentication of the software by the use of cryptographic signing could still be bypassed by changes in the hardware and software. The related key management would mean an extra burden for the election personnel without bringing any benefits.

R.6: *Enhanced controls should be implemented within the software and hardware to restrict access to the services of the system to authorised operators and voters.*

With the current measures in place (See our comments on part 4 of the second report in our letter March 2nd 2006 pages 2 and 3) we do not see the need for these enhanced controls. One should not add complexity for the election personnel when it is not needed.

R.7: *Modifications to the hardware and software components of the system that are necessary to implement the above recommendations should be carried out.*

See our comments on R.6

R.8: *Areas where system documentation is not in conformity with actual hardware and software devices as deployed for use in Ireland should be addressed.*

The documentation should be in conformity with the hardware and software except where general principles are explained, whose implementation can differ in the different voting systems or elections. We would like to clarify the aspects of non conformity with the Independent Test Authority that has performed the analysis on behalf of the Commission.

Usability

R.9: *Usability issues identified by the Commission concerning the interaction between voters and the voting machine interface and that may potentially affect secrecy or accuracy at elections should be addressed.*

We would like to know which usability issues the Commission is referring to.
The full face user interface that is a replica of the paper ballot offers the voter a high degree of "intuitive"

steps to select and review their choices and to cast their votes.
Exit surveys held at the pilots during the Dáil elections of 2002 confirm this. (See enclosure to our letter of March 9th 2006 to the Commission with our comments on part 6, page 1, issue 1 and the enclosure to our letter of February 14th 2006 to the Commission with our comments on part 3, page 3 under usability).

A number of usability issues are mentioned by the Commission, some are minor criticisms (f.i. the "beeps"), some deal with the same breaches of secrecy as the paper voting system and some deal with the way votes are recorded.

Data security

R.10: *The security of sensitive election data (including votes) contained on ballot modules and CDs should be enhanced through the use of encryption (to maintain confidentiality of the data) and cryptographic signing (to detect any attempted alteration).*

Since the risk of attempted access is eliminated by the required procedures that prevent accidental or deliberate loss or damage there is no need for encryption (to maintain the confidentiality of the data) and there is no need for cryptographic signing (to protect against any attempted alteration).

The authentication of the software by cryptographic signing that is checked by the software itself could still be bypassed by hardware and software changes, while the key management associated with encryption and authentication gives an extra burden for the polling staff. (see also our comments on R.5 of Part 8 on page 5 of this letter and on part 4 of the second report in our letter of March 2nd 2006 pages 3 and 4 and our comment on part 6 of the second report of March 9th 2006 pages 2 and 3).

Physical and Operational Security

R.11: *Standard minimum security requirements should be defined and implemented for the storage, set-up, transport and use of voting equipment by returning officers across all constituencies.*

No comment.

R.12: *Specific attention should be paid to the security of programmed voting machines and of ballot modules and CDs containing sensitive election data (including votes) in the periods immediately prior to, during and after the poll.*

We agree.

R.13: *Ballot modules and CDs containing votes cast should be accompanied and/or physically protected from interference at all times while in transit and their movements and transfers of custody should be documented.*

We agree.

R.15: *The existing security arrangements for international transportation of voting equipment between Ireland and Holland by third party carriers and, in particular, the arrangements for collection and distribution to local centres*

in Ireland should be reviewed and enhanced.

In our opinion there is no problem regarding transport between Holland and Ireland.
The shipping agency, the freight companies and sea carrier operate in accordance to the international TAPA standards.
Unaccompanied or unattended voting equipment is stored in sealed containers or in secure areas.

R.16: *A central asset register in electronic format should be established and maintained to record and manage the ownership, location and movement of electronic voting equipment across all constituencies.*

We agree.

Testing

R.18: *Verification of the entire system and the assurance of its suitability for use at elections in Ireland should be sought from a single independent body duly qualified and accredited to carry out the necessary analysis and testing activities.*

The varieties of tests that need to be carried out in a voting system certification process make it likely that more than one Independent Test Authority must be involved. The overview can be the responsibility of one body.

R.19: *The documented requirements and specifications of the system should be independently reviewed to ensure that they provide an adequate expression of its intended purpose and a clear description of its functions against which the system can be independently analysed and tested.*

The Department of the Environment, Heritage and Local Government has the knowledge and the skills to specify the requirements and specifications of the system.

R.20: *Following any modifications of the software and hardware components, rigorous independent analysis and end-to-end testing will be needed to confirm that the system behaves as intended and has no unintended behaviour.*

After any adaptations are made, the VM, PRU, BM and the embedded software are always reviewed and tested by ITA's. This is our standard procedure.

R.21: *Secure methods should be devised, in co-operation with the Manufacturers and the independent testing body, to facilitate rigorous testing of the entire system in ways that the Commission sought to test it but was unable to within the scope of its work.*

We will consider any future proposals of our customer, the Department of the Environment, Heritage and Local Government with a positive attitude.

4. Part 9 Recommendations on Electronic Voting

ELECTRONIC VOTING OPTIONS

Software and Hardware

R.23: *In exploring alternatives to the election management software, the use of open source methods, to an appropriate degree, should be considered as a way to harness and synergise the considerable levels of interest in electronic voting and elections in Ireland with abundant and freely available software engineering expertise.*

We believe that open source methods have a negative impact on voters trust. Since only IT people can review and comment on the software the majority of the people cannot judge for themselves. As there are people who advocate electronic voting and there are those who oppose it, there will not be an objective judgement in this way. The software will always be discredited and the public cannot judge whether this is true or not. In this way mistrust will not be taken away. The best way to ensure voters trust is the analysis and testing of the software by ITA's and if needed, parallel testing before or on Election Day.

R.24: *The feasibility of implementing enhanced levels of audit within the hardware of the chosen system should be explored, including by means of the printer already present in the voting machine or by the further adaptation of the voting machine.*

In our opinion the current audit facilities present within the hardware of the chosen system are adequate. (See enclosure to our letter of March 9th 2006 to the Commission with our comments on part 6, page 14, issue 100).

Specific Secrecy and Accuracy Issues

R.27: Alternative manual vote recording methods (such as optical character recognition and other scanned-in ballot formats) that are compatible with electronic counting methods should be provided for postal voters so that their votes can be incorporated in the electronic count with greater accuracy and secrecy.

No comment.

Accessibility and Voter Options

R.28: *Alternative electronic voting methods should be provided to ensure secrecy and ease of voting across a broader range of voters with disabilities.*

The VM is prepared for an audio device to be connected, which would allow the majority of the visually impaired voters and people with reading difficulties to make use of the VM. (See enclosure to our letter of March 9th 2006 to the Commission with our comments on part 6, page 1, issue 3).

R.29: *The voting machine interface should be modified so as to allow the option of casting blank or null votes uniformly and anonymously as under the paper system.*

The VM has a built-in abstain facility that was de-activated and unlabeled following our customers decision. It needs to be activated and labelled before it can be used.

Requirements, Specifications and Transparency

R.30: *Publication or public inspection of the source code of the chosen system would allow a more open review of the system by computer experts and would facilitate informed debate, greater understanding and confidence in the system among the public as a whole.*

See our comment on R.23.

R.31: *Confidence in the system could be further enhanced by providing a facility for open public testing of the vote recording software and the vote counting software via an on-line web interface designed to simulate the hardware interfaces of the system.*

The best way of enhancing the confidence in the system is to select a number of VM's and PRU's and test them under the supervision of cameras and a notary.

R.32: *Future developments of e-voting in Ireland should be underpinned by a full and formal process of requirements capture and functional specifications for any proposed new system.*

The requirements and the functional specification of the VM, PRU, BM and the embedded software agreed with the Department of the Environment, Heritage and Local Government are formulated in:

- "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

Physical and Operational Security

R.33: *Consideration should be given to the storage of electronic voting equipment on a regional pr provincial basis rather than locally as at present and in preference also to storing it centrally.*

No comment.

ELECTRONIC VOTING CONTEXT

Electronic Voting Standards

R.34: *In the context of future implementations of electronic voting, Ireland should participate, co-operate and contribute more actively in the development of international measures of best practice, guidance and standards in the area of electronic voting.*

No comment.

R.35: *The compliance of electronic voting in Ireland with the non-binding Recommendation Rec (2004)11 of the Committee of Ministers of the Council of Europe should be addressed in the light of areas for improvement and areas of non-compliance identified by the Commission.*

Because test criteria for the Recommendation Rec (2004) are absent, an evaluation of the chosen system with respect to the Recommendation will always be subjective to the interpretation of the general ground rules.
Trying to be as objective as possible we found the VM, PRU, BM and the embedded software in compliance with the Recommendation (see our comments on part 6 of the second report in our letter and enclosure to the Commission of March 9th 2006).

R.36: *Pending the agreement of an internationally agreed standard on electronic voting:*

- *a working Irish standard in accordance with emerging best practice should be developed and adopted.*

The Department has adopted the standards, requirements and best practice methods that are currently applicable for voting equipment and its embedded software in the European countries where electronic voting is in use today.

R.37: *Following the agreement of an internationally agreed standard on electronic voting, and in any case, before the future development of electronic voting in Ireland, provision should be made for the following:*

- *accreditation, by the relevant Irish authorities, of a body or bodies to test and certify electronic voting equipment for use in Ireland in accordance with recognised Irish or internationally agreed standards,*
- *testing and certification, by such body or bodies, of the compliance of such equipment with those standards,*
- *type approval, by the appropriate electoral authorities, for the use in Ireland of electronic voting equipment so certified.*

Where the requirements and standards for the use of VM's in Ireland are derived from the requirements and standards that are defined by the other European countries that use VM's and where the requirements that apply to the specific Irish circumstances are specified by the Department of the Environment, Heritage and Local Government with their expertise and responsibility of conducting elections in Ireland, we are convinced that these requirements, standards and derived test criteria form a sound basis for the development and evaluation of the VM, PRU, BM and embedded software.
The Department has sought accredited ITA's with experience in analysing and testing electronic voting systems. The hardware and software of the VM, PRU and BM were analysed and tested by the accredited German "Physikalisch Technische Bundesanstalt" who is the body that is appointed by German law to analyse and test electronic voting systems before they can be deployed in Germany. (See also the enclosure to our letter of March 9th 2006 to the Commission with our comments on part 6, page 17, issue 112).
The environmental tests including electromagnetic compatibility, electrical tests, temperature tests, shock & vibration tests and drip water tests were carried out by the accredited Dutch TNO. The safety tests were carried out by the accredited Dutch KEMA.

Electoral Administration

R.38: *There should be public consultation on the need for, and expectations of, electronic voting in Ireland and the results of that consultation should inform the future development and deployment of the chosen system or any alternative methods of electronic voting.*

No comment.

R.39: *The development of an electronic register of voters can contribute significantly to the accuracy of elections: however the electronic register should remain separate form electronic voting systems in order to provide continued assurance of voter anonymity in the voting process.*

No comment.

In our comments we have shown that the VM, PRU, BM and the embedded software we supplied are reliable and well suited to their purpose and that they outweigh the paper system. Therefore we strongly encourage its use on short term.

Yours sincerely

Nedap NV

Henk Steentjes

Nedap Comments[84] on Parts 1, 2 and 7

Mr. Alan Murphy Secretary
Commission on Electronic Voting
Floor 4
Setanta Centre
Nassau Street
Dublin 2
Ireland

11th April 2006

Dear Mr. Murphy,

In your letter of March 29th 2006 you invite us to comment on the parts 1, 2 and 7 of the second report of the Commission. We are happy with this opportunity and request that you publish this letter and enclosure in full as part of the report.

You invited Nedap and Powervote individually. We will comment on issues that concern the Voting Machine (VM), the Programming/Reading Unit (PRU), the Ballot Module (BM) and its embedded software.

2 years after the work of the Commission started in March 2004, the Commission is to issue its 2nd report. Part 1 is the introduction, part 2 provides an overview of the Commission's work as presented in parts 3 to 6 and part 7 contains the conclusions, observations and recommendations of the Commission.

1. Part 1 of the second report

We note the positive view of the Commission where it is stated that many of the benefits and advantages that are associated with electronic voting are represented in the chosen system and that the chosen system has the capacity to deliver enhanced levels of accuracy and acceptable similar levels of secrecy when compared with paper voting in Ireland.

The Commission does not yet recommend the use of the system because it is as yet unproven in practice at national elections in Ireland and because the Commission is of the opinion that the reliability and trustworthiness of the chosen system are as yet unproven by the analysis and testing carried out to date.

Where the Commission concludes in the comparative assessment of the chosen system and the paper system that the secrecy risks are low (Part 5) and where the Commission concludes that the risks to accuracy in the chosen system are fewer and of lower magnitude than in the paper system (based on the assumption that the reliability and trustworthiness are proven) (Part 5) it comes down to the questions:

a) *How can the reliability and trustworthiness of the chosen system be proven?*

[84] At the request of Nedap, these comments have been reproduced by the Commission in the form they were received, subject only to the deletion of page references as they relate to earlier drafts of the Commission's report. The comments also refer to text contained in earlier drafts that has been revised in the final version of the report.

b) How can voters trust in electronic voting be established?

How can the reliability and trustworthiness of the chosen system be proven?

- *Testing against clear defined specifications and standards*

When the Commission is of the opinion that the specifications and standards that were agreed in 2003 should be amended, then it is possible that as a result of these new specifications and standards the system should be adapted and additional tests should be performed.
However, the Commission does not indicate in its second report where and why there should be deviation from the specifications and standards that were agreed in 2003.

It is remarkable that the Commission nonetheless concludes that the reliability and trustworthiness are as yet unproven by the analysis and testing carried out to date, although all EMS system components were independently tested on behalf of the Department by ITA's for compliance with the requirements of 2003.
By not incorporating this in its evaluations the Commission unintentionally contributes to the undermining of voters trust in the chosen system.

- *End to end testing*

Supplemental to the above end to end testing can be introduced. This means that a number of complete election scenarios are tested, at which the procedural side also gets the necessary attention.

How can voters trust in electronic voting be established?

- *"Quality seal" for electronic voting systems*

Voters cannot see what happens inside a VM. A "quality seal" for electronic voting systems by clear regulations regarding the design, the analysis and testing that voting systems have to meet before they can be deployed, creates the necessary confidence. This is the situation in the European countries where electronic voting is applied today.

Where the requirements and standards for the use of VM's in Ireland are derived from the requirements and standards that are defined by the other European countries that use VM's successfully for many years and where the requirements that apply to the specific Irish circumstances are specified by the Department with her expertise and responsibility of conducting electrons in Ireland we are convinced that these requirements, standards and derived test criteria form a sound basis for the development, evaluation and testing of the VM, PRU, BM and embedded software.

- *Parallel testing on Election Day*

It is important that voters can see that their preferences are accurately recorded and actually taken into account at the count.
Probably most of the voters trust that certified VM's accurately record their preferences.
In order to convince also those voters who think that VM's are possibly tampered with, parallel testing can be a solution.

On Election Day a number of randomly chosen VM's that are prepared for the election are taken. Under the watchful eyes of the public (via cameras) and a notary, known votes are cast on these VM's and these are compared with the result. In this way it is evident for all voters that the VM's accurately record preferences and that these preferences are actually counted.

2. Part 2 of the second report

In part 2 the Commission explains its approach to its work being the consideration of the secrecy and accuracy of the chosen system, the review of the testing carried out and the comparative assessment of the chosen system and the paper system.

Since we discussed the analysis and testing above, we now shortly address the situation in the USA and the 2004 Recommendation Rec(2004) by the Committee of Ministers of the Council of Europe.

a) Electronic Voting in the USA

The Commission concludes that there is a significant "climate change" with regard to electronic voting, being *"significant alterations in the levels of public and political expectation and acceptance of electronic voting, both in Ireland and abroad"* (part 2).

The climate change did not originate from Europe but from the USA.
The problems with outdated voting systems became apparent in the Presidential elections of 2000. In an answer on that new electronic voting systems were introduced, systems that were mainly based on a PC platform with a Windows operating system. Various states have attempted to solve the concerns with regards to the integrity of the voting equipment by the provision of a Voter Verifiable Audit Trail. In our opinion this provision does not enhance voters trust, it rather achieves the opposite. (See our letter of March 20th 2006 with our comments on part 5, enclosure 1 pages 1 and 2)

b) Common standard on electronic voting in Europe

The Commission concludes that "*there are clear signs of movements towards a common standard on electronic voting with the adoption in 2004 of a Council of Europe Recommendation on legal, technical and operational aspects of electronic voting"* (part 2).

The Recommendations Rec (2004) of the Committee of Ministers of the Council of Europe have the character of basic principles. They are developed in order to harmonize the basic principles in all European countries. They do not aim at being used as a direct means for performing tests, in particular, against which a specific system is tested. Such testable requirements must still be developed. In Ireland the "Requirements for voting machines for use at elections in Ireland DVREC-2" of March 5, 2003 are such requirements. Once such testable requirements have been developed, they shall not contradict the basic principles. This is the aim of the Recommendations Rec (2004).

3. Part 7 of the second report

a) Summary of conclusions

There are a number of issues where our opinion differs from that of the Commission.
In this respect we refer to our comments on part 1 and part 2 in this letter and our comments on the parts 3, 4 5 and 6 of the second report respectively. They include:

- *Reliability and trustworthiness of the chosen system*

In our opinion a "quality seal" for electronic voting systems by clear regulations regarding the design, the analysis and testing that voting systems have to meet before they can be deployed, creates the necessary confidence. This can be complemented by parallel testing. (See our comment on part 1 earlier in this letter)

- *Technical aspects and testing*

As we have shown in our comments on part 3 of the second report in our letter and enclosure of February 14th 2006 the requirements, standards and test criteria that were applicable for the design, evaluation and testing of the VM, PRU, BM and the embedded software are adequate with respect to electronic voting practices in Europe, which were developed over the last decades and we have shown that the evaluation and testing done by the ITA's have proven satisfactorily that these components of the chosen system provide the necessarily secrecy and accuracy when the proper procedures are applied.

- *Physical and operational security aspects*

We show in our comments on part 4 of the second report in our letter March 2nd 2006, that further work should address the procedural side of the election process.

- *Comparative assessment*

We show in our letter and enclosures of March 20th 2006, containing our comments on part 5 of the second report, that the VM, PRU, BM and the embedded software outweigh the paper system in terms of accuracy, secrecy and the other important criteria mentioned in part 5 of the Commission's second report.

- *E-voting best practice: Council of Europe Recommendation*

See our comments on page 3 of this letter.
Because test criteria are absent, an evaluation of the chosen system with respect to the Recommendation will always be subjective to the interpretation of the basic principles.
Trying to be as objective as possible we found the VM, PRU, BM and the embedded software in compliance with the Recommendation (see our comments on part 6 of the second report in our letter and enclosure to the Commission of March 9th 2006).

b) Overall conclusion

We note some highlights from the Commissions overall conclusion.

- *The proposed operational arrangements, the official tests and validation undertaken to date are insufficient to provide the requisite levels of confidence.*
- *This conclusion is not based on any particular finding that the system will not work, but the operation to the desired secrecy and accuracy levels is not yet proven.*
- *When the recommendations of the Commission are met then it is likely that the chosen system can be deployed and used with confidence in the future.*

We refer to our comment on part 1 on pages 1 and 2 of this letter.

It is remarkable that the Commission concludes that the official tests and validation undertaken to date are insufficient to provide the requisite levels of confidence, although all EMS system components were independently tested on behalf of the Department by ITA's for compliance with the requirements of 2003.

c) Recommendations

On a number of important issues we have a different opinion than the Commission. In our comments to the Commission on the second report we have proposed alternatives where applicable. Eventually it will be up to the Irish Government to

decide how to proceed with electronic voting in Ireland. We will consider any future proposals of our customer, the Department of the Environment, Heritage and Local Government with a positive attitude.

In the enclosure we comment on the Commissions recommendations where applicable for the VM, PRU, BM and the embedded software.

We hope that the comments which we present in this letter, just like our comments on the other parts of the second report can convince the Commission that the VM, PRU, BM and the embedded software are adequately designed, analysed and tested and that their use in combination with the right procedures is preferred over the use of the paper based system of voting with its related problems regarding secrecy and accuracy.

We recommend the use of the system on short notice in a limited number of constituencies in Ireland, following the thorough investigations carried out by the ITA's and the Commission on Electronic Voting. This will present a strong signal to the Irish voters to enhance voters trust.

Yours sincerely

Nedap NV

Henk Steentjes

Encl.: Detailed comments on the recommendations in part 7 of the second report of the Commission

Nedap Comments[85] on Part 3

Mr. Alan Murphy Secretary
Commission on Electronic Voting
Floor 4
Setanta Centre
Nassau Street
Dublin 2
Ireland

Groenlo, 14th February 2006

Dear Mr. Murphy,

In your letter of January 17th you invite us to comment on part 3 of the second report of the Commission. We are happy with this opportunity and request that you publish this letter and enclosure in full as part of the report.

We will react on the Voting machine, the Programming Reading Unit and the Ballot module with their hardware and embedded software.

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

Ease of use for election personnel and voters
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 the EMS where we follow the administrative electoral procedures currently in place for paper based voting.
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.

The value of this was recognised by the Commission in its first report (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*".

[85] At the request of Nedap, these comments have been reproduced by the Commission in the form they were received, subject only to the deletion of page references as they relate to earlier drafts of the Commission's report. The comments also refer to text contained in earlier drafts that has been revised in the final version of the report.

Difficult to maliciously introduce large numbers of votes

The stand alone design and the proprietary hardware and proprietary software of our VM, PRU and BM makes it difficult for anyone to tamper with them.

The Commission's statement underlines this:

"*the Commission was unable to exercise the ballot module and other downstream components of the system using large numbers of known votes introduced authentically using a test harness, either to bypass the voting machine interface or to introduce them directly onto the ballot module itself. Although this was a limitation on the Commission's proposed work, it also represents a significant strength of the system. It shows the degree of difficulty presented to anyone seeking maliciously to introduce large numbers of votes to the system at an election, via either a voting machine interface or a ballot module*".

Election Management System for Ireland designed, tested and delivered according agreed specifications of 2003

The EMS for Ireland was designed and delivered in accordance with the specifications and contracts as agreed with DOEHLG in 2003.

For the VM, PRU and BM 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.

All EMS system components were independently tested for compliance on behalf of DOEHLG.

The VM, PRU and BM hardware and embedded software were tested by the German Independent Test Authority "Physikalisch Technische Bundesanstalt" (PTB).

Important to mention is that the PTB did the static analysis on the VM and PRU internal embedded C-code software and did the manual source code inspection asked for in part 3 of the Commission's second report by which potential run-time errors were discharged.

We do not see why this should be repeated by the Commission.

The environmental tests including electromagnetic compatibility, electrical tests, temperature tests, shock & vibration tests and drip water tests were carried out by the accredited Dutch TNO. The safety tests were carried out by the accredited Dutch KEMA.

We do not see why this should be repeated by the Commission.

Two years after the work of the CEV started in march 2004, the CEV is to issue its 2nd report. In part 3 of this second report the Commission makes further judgements on the technical aspects and testing of the chosen system.

After reading part 3 we must conclude that in two years of evaluation and additional testing the Commission did not find any substantial flaws.

Commission seeks for new specifications and standards

From reading part 3 of the second report we must conclude that, whereas the VM, the PRU and the BM hardware and embedded software is designed, tested and delivered according the above mentioned specifications as agreed with DOEHLG in 2003, the Commission is seeking new standards and specifications to judge the chosen system.

We do not see an analysis of the agreed specifications and we do not see a clear definition of amended specifications.

If the agreed specifications of 2003 are not adequate to support elections in a trustworthy way, we invite the Commission to specify why not and what amendments should be made.

Recognised standards for electromagnetic compliance tests
We note that the Commission seeks for recognised standards for electromagnetic performance tests (Standards), saying "There is currently no international standard for the electromagnetic compliance testing of electronic voting equipment".
We comment: In the Netherlands, Germany and France there are standards for compliance testing, also for electromagnetic compliance testing, of electronic voting equipment, which were adopted by the DOEHLG in their "requirements for voting machines for use at elections in Ireland DVREC-2" of March 5, 2003. The voting machines, programming reading units and ballot modules were tested accordingly by Independent Test Authorities (ITA's).

Extended Ballot module test at 7 Tesla
The extent of the tests done by the Commission is sometimes almost without limit.
We note that the Commission states: "In this test, a ballot module containing data was exposed to a very strong electromagnetic source of 7 Tesla. Following this exposure, the contents of the module was found to be unaffected".
"Equipment to produce a magnetic field of this strength is in no sense portable or widely available, requiring a large and very expensive installation". This test was already done by the Commission in the work reported in their first report.

Even in MRI-scans the magnetic field strength is limited to 2,5 Tesla because of the danger for the patients to develop cancer when higher field strengths are applied.
The test is like using a sledge hammer to test the ruggedness of a plastic case.

Testing against clear defined specifications and standards
When the Commission is of the opinion that the specifications and standards agreed in 2003 should be amended, then it is possible that as result of these new specifications and standards the system should be adapted and additional tests should be performed.

Testing without clear defined specifications sets no limit to the time and amount of tests and is not an objective way of judging a system.

We will comment on the main conclusions as follows:

HARDWARE
"The main hardware components of the system, namely the voting machine, the programming/reading unit and the ballot module are of good quality and design. They are robust against failure and are generally well suited to their purpose. Further investigation, refinement, testing and independent certification of these components would however be necessary before they could be confidently recommended for use at elections in Ireland".

We take notice of the fact that the Commission finds the VM, the PRU and the BM of good quality and design and that they are robust against failure and are generally well suited to their purpose.
The VM, the PRU and the BM have been tested by ITA's according the specifications as agreed to with DOEHLG.

Further investigation, refinement, testing and independent certification is only meaningful if the Commission defines why the existing specifications are not sufficient and what amendments should be made.

SOFTWARE

"The embedded C code software within the voting machine and programming/reading unit is of an adequate standard and, while it is not of mission critical standard, there is evidence to suggest that it has been developed according a recognisable structured design process which is broadly in accordance with industry best practice. Further investigation of its behaviour, followed by refinements of its functions, further testing and independent certification would be necessary before its trustworthiness could be confirmed for use at elections in Ireland. ".

We take notice of the first part of the conclusion of the Commission. We note that the embedded software in the voting machine, the programming/reading unit and the ballot module has been evaluated and tested by the German "Physikalisch Technische Bundesanstalt" according the specifications as agreed to with DOEHLG
Important to mention is that the PTB did the static analysis on the VM and PRU's internal embedded C-code software and did the manual source code inspection asked for in part 3 of the Commissions second report by which potential run-time errors were discharged.

Further investigation, refinement, testing and independent certification is only meaningful if the Commission defines why the existing specifications are not sufficient and what amendments should be made.

DATA/PERIPHERALS

While the ballot module is robust and generally well suited to its purpose, the measures for ensuring the security of the data stored on it are not of a sufficient standard. The use of data encryption and cryptographic signing of this data would enhance the levels of security and give greater confidence in the integrity of the system.

We take notice of the fact that the Commission finds the ballot module robust and generally well suited to its purpose. On the wish for encryption it is our view that the secure key-management that is associated with cryptography adds to complexity of the election process whereas the risks can be neutralized by proper procedures as is the case when transporting ballots in the paper based system.
We must never forget that the infrequent nature of elections make it mandatory to keep the process simple and easy to understand in practical use for election personnel and voters. Therefore we follow the administrative electoral procedures currently in place for paper based voting, the VM is based on a "booth" design and offers a replica ballot interface. This makes the system easy to work with for the election personnel and the voters

TESTING

The testing of the system as a whole carried out to date, as well as the investigation, analysis and independent testing and certification of its individual components, is insufficient to provide a secure basis for the use of the system at elections in Ireland. While the Commission's work has laid the foundations for this process, considerably more work will be required in this area.

The chosen system was tested by Independent Test Authorities against the agreed specifications of DOEHLG. Where applicable they were derived from standards for voting systems in use for years in the Netherlands, Germany and France.

When the Commission is of the opinion that the specifications and standards agreed in 2003 should be amended, then it is possible that as result of these new specifications and standards the system should be adapted and additional tests should be performed.
We do not see an analysis of the agreed specifications and we do not see a clear definition of amended specifications.

Testing without clear defined specifications sets no limit to the time and amount of tests and is not an objective way of judging a system.

Conclusion

After reading part 3 we must conclude that in two years of evaluation and additional testing the Commission did not find any substantial flaws in the VM, PRU and BM hardware and embedded software of the chosen system. Therefore we do not see any reason why to postpone the use of the chosen system

With the proper procedures in place the secrecy of the chosen system is guaranteed and since its accuracy is much higher than in a paper based system the benefits are clear.

We therefore strongly encourage the use of the chosen system. An election in a moderate number of constituencies would be a great start.

Yours sincerely

Henk Steentjes

Nedap NV

Encl.: Detailed comments on part 3 of the second report of the Commission on Electronic Voting.

Detailed comments on part 3 of the second report of the Commission on Electronic Voting.

3.2.1 The Voting Machine
(b) Desk Review of the Voting Machine

Potential vulnerabilities of the voting machine identified in the course of this review as having a bearing on secrecy or accuracy were reviewed by the Commission and, where appropriate having regard to security and confidentiality considerations, these vulnerabilities are reflected in the Commissions findings, listed further below. It should be noted that these potential vulnerabilities have not generally been assessed or ranked by the Commission according to their likelihood of occurrence at this time.

In judging vulnerabilities or risks the question is always what risks are tolerable or acceptable. Likelihood of occurrence (probability) and impact must be defined to compare the chosen system with the current paper system.

(c) Technical Testing of the Voting Machine

Standards: There is currently no specific international standard for the electromagnetic compliance testing of electronic voting equipment. However, even though the threats to such equipment are not currently well defined, a number of existing standards are nonetheless appropriate and applicable in the context of the public environment in which such equipment may be used at elections. The Commission's testing of the system was designed to meet or exceed these standards.

In the Netherlands, Germany and France there are standards for compliance testing, also for electromagnetic compliance testing, of electronic voting equipment, which were adopted by the DOEHLG in their "requirements for voting machines for use at elections in Ireland DVREC-2"of March 5, 2003. The VM, PRU and BM were tested accordingly by Independent Test Authorities (ITA's).

We would like to know from the Commission what the standards are that the VM was tested against.

Guidance to users of the machine: It was also noted that the system manuals and official guidelines for deployment and use of the voting machine contain no information about its electromagnetic performance and offer no specific guidance on the need to locate the equipment away from potential sources of intentional or unintentional electromagnetic interference.

Election personnel should not have to worry about electromagnetic interference. That is why the VM is in a high degree invulnerable to electrostatic discharge or RF signals and there is no need for specific guidance on this point.

(d) Principal Findings Concerning the Voting Machine

Reliance on Voters and/or Operators to Detect Faults
The vast majority of voters must vote alone and unaided. Voters will have a wide range of ages, abilities and levels of technical competence. All voters will be unfamiliar with the voting machine, at least during the first elections in which it is used. It is quite likely, furthermore, that voters will not detect failures of the voting machine that may occur during polling and this is something that cannot be mitigated by voters education policies. Any system of electronic voting must

therefore be designed in a way that does not compromise the accuracy with which the views of even the lest able voters are recorded.

Errors are very infrequent, so we have the VM halted and a specific error code appears in the displays of the machine. No further action can take place and this will be noticed by the voter and the operator of the control panel who reports the error code to the help desk. The error code is directly understood by the people on the help desk and appropriate action can be taken. Our experience in the various countries where our systems are deployed is that voters of different ages and also first time voters can handle such a situation. It is also our experience that the polling staff with clear and simple instructions can also handle these situations.

Other Hardware Vulnerabilities
The Commission's analysis also indicates a further potential vulnerability that may arise from a feature of the system designed to facilitate voting by visually impaired persons via a physical external data link, which remains present but unused within the voting machine in its Irish application. Taken with the existence of the corresponding embedded C code software within the voting machine to control this link, serious questions arise as to the effectiveness with which the functioning of this feature has been fully deactivated for its intended, or possibly unintended, use.

This data link can only be activated when the Visual Impaired Device (VID) is connected to this port. The activation is done by depressing the VIS button on the control panel. The voting machine checks the presence of the VID before the data link becomes active.

Given the fact that the the voting machine and the PRU contain the same main board and embedded C software the fear of the Commission is that:
"If so, this has the serious implication that an attacker with access to a single voting machine and the appropriate technical knowledge could adapt this to program a large number of ballot modules"

This malicious attacker then has to do something with these programmed BM's. Programmed BM's contain no votes, but do contain the names of the candidates. If such an attack would take place on VM's already prepared for an election the candidates in the BM would be replaced by others. This can be detected before the VM is released for voting. This is comparable with the substitution of paper ballots papers by false ones, which is much easier to do.

Large scale fraud with votes is very unlikely. As the Commission reports:
"*the Commission was unable to exercise the ballot module and other downstream components of the system using large numbers of known votes introduced authentically using a test harness, either to bypass the voting machine interface or to introduce then directly onto the ballot module itself. Although this was a limitation on the Commission's proposed work, it also represents a significant strength of the system. It shows the degree of difficulty presented to anyone seeking maliciously to introduce large number of votes to the system at an election, via either a voting machine interface or a ballot module*".

Software and Hardware Security: Access Controls

Only physical security measures such as keys, tamper detection seals and other design features have been applied, but no additional security measures such as password or other code protections have been implemented.

The management and application of passwords would mean an extra burden on the polling staff. Since we want to keep the election process as simple as possible we rely on physical security measures which in our vast experience have proven to be adequate.

Usability: Ballots that do not Reflect the Intentions of the Vote
Six remarks are made.
Usability: Interfering Voter Behaviour from Voting Machine
Three remarks are made.

The behaviour of the VM is defined in the "Functional specification – Nedap voting system ESI2 – Powervote version 1.9" of May 5, 2003 that was agreed with DOEHLG.
The beeps generated when preferences are selected referred to can be switched off (option while programming the BM). In this way beeps say nothing about the preferences that votes select.

3.2.2. The Ballot Module

(c) Technical Testing of the Ballot Module
Electromagnetic Susceptibility and Compliance

In this test, a ballot module containing data was exposed to a very strong electromagnetic source of 7 Tesla. Following this exposure, the contents of the module was found to be unaffected.
Equipment to produce a magnetic field of this strength is in no sense portable or widely available, requiring a large and very expensive installation.

Even in MRI-scans the magnetic field strength is limited to 2,5 Tesla because of the danger for the patients to develop cancer when higher field strengths are applied.
The test is like using a sledge hammer to test the ruggedness of a plastic case.

Principal Findings Concerning the Ballot Module
Although simple and very short checksums are applied to some of the data on the Ballot module, confidence in the secrecy of the ballot would be greatly enhanced if the data was protected from unauthorised access and disclosure by the cryptographic methods mentioned above, which are standard ways of protecting any sensitive electronic information.

The strong checksums are used for the detection of corrupted data. These checks are performed at any time data is read or votes are stored.
It is our view that secure key management that is associated with cryptography adds to complexity of the election process, whereas the risk can be neutralised by proper procedures.

Volume Testing
We note:
The Commission was unable to exercise the ballot module and other downstream components of the system using large numbers of known votes introduced authentically using a test harness, either to bypass the voting machine interface or to introduce them directly onto the ballot module itself. Although this was a limitation on the Commission's proposed work, it also represents a significant strength of the system. It shows the degree of difficulty presented to anyone seeking

maliciously to introduce large number of votes to the system at an election, via either a voting machine interface or a ballot module.

3.2.3. The Programming/Reading Unit

(c) Technical Testing of the Programming Reading Unit

The need for such testing was also highlighted in the Commissions first report which noted the very significant shortcoming that the programming/reading unit had not been independently tested.

As we have commented on the first report (page 414) the software of the PRU is part of the software package for the VM that is tested by the PTB. The communications is tested. Only defined items are transferred. The reading of votes is implicitly tested by source code analysis and source code inspection.

Hardware Vulnerabilities – electromagnetic Eavesdropping and Interference
It was noted that no specific operator guidance is given on positioning the device so as to minimise its susceptibility to electromagnetic threats at elections, whether intended or unintended.

Election personnel should not have to worry about electromagnetic interference. That is why the VM is in a high degree invulnerable to electrostatic discharge or RF signals and there is no need for specific guidance on this point.

Reliance on Embedded Software
An important example of how the software may behave in response to unintended inputs was discovered in testing carried out by the Commission, whereby a simple but unexpected command caused the programming/reading unit to halt. This raises concerns over the Quality of the embedded C code software and the level of testing performed on it.

The PRU software is purposely designed to halt when an unexpected command is received. The only way of recovery from this is to switch off the PRU and switch it on again. If this occurred when a ballot module was programmed, it now has to be reprogrammed. If votes were read in, the read in action has to be done again.

3.3.1 Embedded Software (C code)

Software quality
We note:
The analysis for the source code itself did not uncover any major functional failures

A software project management plan was not supplied.

Here we do not agree. We did supply to QinetiQ the project overview of the development of the ESI2 voting machine embedded software with details on the software conventions.

Some useful documentation has been supplied on the design, specification, development and quality of the software, although its accuracy in relation to the actual source code is questionable.

Here we no not agree. We did supply to QinetiQ the technical documentation of the hardware and the embedded C software. This covers the requirements, the software design and the software test plan and the documented software tests that were performed.
We would like to know from the Commission where the documentation is not in correspondence to the source code.

Version control appears to be inadequate as the version numbers are not common across the code and the procedures to find and change the embedded version number is not documented, which means it cannot be quickly or easily checked.

Here we do not agree. The version control was maintained throughout the project. Some software modules have higher version numbers than others while they are addressed more often than others, but this the nature of version control. The version control method is very straightforward and easy to work with.

We note:
The clarity of the code is adequate, although some parts are easier to understand than others.

We note:
One of the three parts of the code is logically structured, with sensible functional layers. The remaining two parts are less so, but justifiably so because the functionality of the code in these parts is less complex.

The automated analysis found no potential divide by zero errors, but did find a significant amount of other potential runtime errors present in the code. The significance of these can only be determined by further analysis and it is likely that many of them will be discharged as false concerns.

The embedded C software was tested by the accredited German PTB. They performed automated analysis and **performed a manual source code inspection of the C code by which the potential runtime errors were discharged.** Owing to the documentation of each individual test scenario in test protocols, which are archived at the PTB, each of the tests performed in the Software Testing Laboratory is repeatable. The testing method used and the testing procedure applied belong to the information laid down in protocols.
We do not see why this has to be repeated again.

Architecture
The incorporation, within the C code on the main board, of functionality relating to both the voting machine and the Programming/reading unit represents an inadequate segregation of functions. A consequence of this is that either function may be susceptible to changes made in the other and both would have to be retested as a result of any such change.

Here we do not agree. **It is a great benefit that the functions for reading and interpreting votes in the VM and the PRU are done by the same software modules.** The software is well structured, that means that when changes apply to one module it has no effect on others.

3.5 Summary of Findings on Technical Aspects and Testing
3.5.1 Specifications and Requirements capture
There is little evidence that a formal and rigorous process of specification and requirements capture was applied to

support the adaptations and development of the software components of the system for use in Ireland. This is inconsistent with software engineering best practice and falls significantly short of the standard that would be required of a system that has been deemed by the Commission to be mission critical.

We do not understand this. The requirements for the VM, PRU and BM we discussed with DOEHLG and were laid down in "Requirements for voting machines for use at elections in Ireland DVREC-2" of March 5, 2003.
The requirement for the functionality of the VM, PRU and BM was during the development process discussed with DOEHLG and was laid down in "Functional specification – Nedap voting system ESI2 – Powervote version 1.9" of May 5, 2003.
No adaptation to the system or of the systems functionality was made before new specifications were agreed. This method was rigorously applied during the development stage.

From this perspective we do not understand why the Commission did not analyse the agreed specifications and has no clear definition of amended specifications.
Testing without clear defined specifications sets no limit to the time and amount of tests and is not an objective way of judging a system.

3.5.2 Documentation
.. while the documentation in respect of the voting machine hardware and software components does not fully correspond to the configuration of these components as they would be deployed for use in Ireland.

Here we no not agree. We did supply to QinetiQ the technical documentation of the hardware and the embedded C software. This covers the requirements, the software design and the software test plan and the documented software test that were performed.
We would like to know from the Commission where the documentation is not in correspondence to the source code.

3.5.3 Design and Development Process
A recognisable structured design process, broadly in accordance with industry best practice, was nonetheless deployed in the design and development of the embedded C Code software, but without sufficient independent review and testing.

The VM, PRU and BM hardware and embedded software were tested by the German Independent Test Authority "Physikalisch Technische Bundesanstalt" (PTB), including a full source code review.
Important to mention is that the PTB did the static analysis on the VM and PRU internal embedded C-code software and did the manual source code review asked for in part 3 of the Commissions second report by which potential run-time errors were discharged. Owing to the documentation of each individual test scenario in test protocols, which are archived at the PTB, each of the tests performed in the Software Testing Laboratory is repeatable. The testing method used and the testing procedure applied belong to the information laid down in protocols. The full test report has been made available.
We do not see why this should be repeated by the Commission.

3.5.4. System maintenance
The design, development and documentation processes are generally inadequate in relation to software engineering best practice and falls significantly short of that required for mission critical systems.

We are astonished. The Commission states: A recognisable structured design process, broadly in accordance with industry best practice, was nonetheless deployed in the design and development of the embedded C Code software, but without sufficient independent review and testing.
The Commission states: The embedded C code software within the voting machine and programming/reading unit is of an adequate standard and, while it is not of mission critical standard, there is evidence to suggest that it has been developed according a recognisable structured design process which is broadly in accordance with industry best practice.

3.5.8. Software authentication
Another major vulnerability for the system arises from the absence of any software mechanism within the system, or any formal and independent software authentication process outside it, to endure and verify that the embedded software installed on all voting machines and programming /reading units and the election management software used to administer the election is indeed the correct version that has been independently tested and certified and that has been approved for use by the electoral authorities.

We do not agree. As we have explained in our letter of January 6th 2006 to the Commission both the VM and the PRU check the correctness of the program software in their program memories. A sum check is performed at start up and compared with the stored checksums. In case of a difference an error message is displayed. In the FUNCTIONS mode in the VM there are options to show (menu “versions and checksums”) the versions and the checksums of the program software in the Main Board, the Connection Board and the Display Boards on the VM display and they can be printed by the internal printer (menu “print settings”).
PRU: In IES the status of the PRU can show the software version number.

3.5.10 Testing
Review of previous testing
The Commission concluded in its first report that the level and comprehensiveness of the testing of the system carried out to date are insufficient to establish the trustworthiness and reliability of the system. As the Commission has not been advised that any further official or independent testing has been carried out in the interim, this conclusion continuous to be applicable in respect of the chosen system.

After reading part 3 we must conclude that in two years of evaluation and additional testing the Commission did not find any substantial flaws.

The EMS for Ireland was designed and delivered in accordance with the specifications and contracts as agreed with DOEHLG in 2003.

For the VM, PRU and BM 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.

All EMS system components were independently tested for compliance on behalf of DOEHLG.
The VM, PRU and BM hardware and embedded software were tested by the German Independent Test Authority “Physikalisch Technische Bundesanstalt” (PTB).

Important to mention is that the PTB did the static analysis on the VM and PRU internal embedded C-code software and did the manual source code inspection asked for in part 3 of the Commission's second report by which potential run-time errors were discharged.

We do not see why this should be repeated by the Commission.

The environmental tests including electromagnetic compatibility, electrical tests, temperature tests, shock & vibration tests and drip water tests were carried out by the accredited Dutch TNO. The safety tests were carried out by the accredited Dutch KEMA.

We do not see why this should be repeated by the Commission.

We do not see an analysis of the agreed specifications and we do not see a clear definition of amended specifications.

If the agreed specifications of 2003 are not adequate to support elections in a trustworthy way, we invite the Commission to specify why not and what amendments should be made.

Testing without clear defined specifications sets no limit to the time and amount of tests and is not an objective way of judging a system.

Nedap Comments[86] on Part 4

Mr. Alan Murphy Secretary
Commission on Electronic Voting
Floor 4
Setanta Centre
Nassau Street
Dublin 2
Ireland

2 March 2006

Dear Mr. Murphy,

In your letter of February 17th you invite us to comment on part 4 of the second report of the Commission. We are happy with this opportunity and invite you to publish it as part of the report.

You invited Nedap and Powervote individually and we will comment on issues that concern the Voting Machine (VM), the Programming/Reading Unit (PRU), the Ballot Module (BM) and its embedded software.

Our conclusion on part 4 of the second report

The physical and operational security aspects of the VM, PRU, BM, the embedded software and the procedures in place at the Manufacturers addressing the physical and operational security aspects with the manufacture and transport are of adequate standard. The findings for the security policy management that require attention are equally important for the current paper bases system.
With the proper procedures in place associated with transport, storage and deployment for use the system is ready for use at elections in Ireland.

Where the testing of the hardware and software shows that no substantial failures have been detected, further work should address the procedural side of the election process and not the testing of the election hardware and software.

The Election management System

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. Ease of use in combination with transparency has always been the guiding principle in the development of voting systems.

[86] At the request of Nedap, these comments have been reproduced by the Commission in the form they were received, subject only to the deletion of page references as they relate to earlier drafts of the Commission's report. The comments also refer to text contained in earlier drafts that has been revised in the final version of the report.

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.
The stand alone design and the proprietary hardware and proprietary software of our VM's, PRU's and BM's makes it difficult for anyone to tamper with them.

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

For the VM, PRU and BM 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.

All EMS system components were independently tested for compliance on behalf of DOEHLG.
The VM, PRU and BM hardware and software were tested by the German independent test institute "Physikalisch Technische Bundesanstalt" (PTB), including a full source code review and source code inspection.

The environmental tests including Electromagnetic Compatibility, electrical tests, temperature tests, shock & vibration tests and drip water tests were carried out by the accredited Dutch TNO. The safety tests were carried out by the accredited Dutch KEMA.

Part 4 of the second report

2 years after the work of the CEV started in March 2004, the CEV is to issue its 2nd report. In part 4 of this second report the Commission evaluates the physical and operational arrangements concerning the manufacture, transportation, storage and use of the chosen system are reviewed in the light of recognised standards applicable to information security management systems.
The reference was the Irish national standard on information security management systems IS1799 -2:2002 - Part 2 Specification an Guidance for Use.

We note the Commission's findings:
Nedap has sought to adopt best practice in terms of preventing unauthorised access to its premises and secure areas and sufficient controls appear to be in place to prevent unauthorised third parties from gaining access to the development, manufacturing and assembly facilities at which the hardware and embedded software components of the chosen system are produced.

Storage and Custody During Elections
Once programmed, each voting machine has the combined sensitivity of an empty ballot box and a number of blank ballot papers. While the same sensitivity also exists under the paper system, segregation of empty ballot boxes and blank ballot papers (usually locked within one or two ballot boxes until the day of the election) is more easily achieved and proven. There are also additional sensitivities of the programmed voting machine and its configuration that do not exist under the current paper system.

There are measures in place on the VM to secure the VM against these risks. There are seals on the electronic cabinet,

a lock on the user panel and a seal on the programmed BM in the VM. The integrity of the candidate names and the layout on the voter panel as programmed in the BM can be checked against the names and layout on the Ballot on the voters panel of the VM and the BM can be checked prior to the start of the poll to ensure that no votes are stored. This can be printed in the open poll statement and be time stamped by the presiding officer. The VM's ID and the software version and checksums are also printed on the open polls statement. Together these measures provide a strong means of detecting if unauthorised access to the VM has taken place.

Findings on Physical and Operational Security

Manufacture and Transport

There is however a critical reliance of Nedap's hardware and embedded software components on the availability and reliability of the election management software developed by Groenendaal B.V. and supplied by Powervote Ireland such as that any loss or failure of that software could render the Nedap components of the chosen system unusable beyond the control of Nedap.

In order to deal with the situation of loss of the election management software the election management software is placed under escrow to ensure continuity.
In addition DOEHLG was given an option to purchase the IES-Ireland software, so that it could be under the direct control of DOEHLG.

There is a potential risk to the security of voting equipment (hardware and embedded software) that is unaccompanied and/or unattended while in transit from the Manufacturers by road and sea internationally and also during local delivery to individual Returning Officers.

The shipping agency that selects the freight companies and sea carrier works according the international TAPA standards. Unaccompanied or unattended voting equipment is stored in sealed containers or in secure areas.

Use at Elections

*The transport of the ballot module from the polling station to the read-in and count centre is the most sensitive stage in the entire life-cycle process of the chosen system. There is a low risk associated with the main theoretical threat of the substitution of a ballot module that has been programmed with bogus votes by a person with access to the election management software and a programming/reading unit. However there are also the threats of accidental or deliberate damage, destruction or loss of the ballot module which, notwithstanding the existence of a backup ballot module, can have an impact on confidence in the electronic voting syste*m.

The main theoretical threat of substitution of a ballot module with one that has been programmed with bogus votes is also confirmed several times in Part 3 of the second report. We refer to the finding of the Commission in Part 3: *the Commission was unable to exercise the ballot module and other downstream components of the system using large numbers of known votes introduced authentically using a test harness, either to bypass the voting machine interface or to introduce then directly onto the ballot module itself. Although this was a limitation on the Commission's proposed work, it also represents a significant strength of the system. It shows the degree of difficulty presented to anyone seeking maliciously to introduce large number of votes to the system at an election, via either a voting machine interface or a ballot module.*

Since the risk of substitution of a ballot module with one that has been programmed with bogus votes is mainly

theoretical and can be mitigated even further by physical security measures that mitigate the risk of accidental or deliberate damage, destruction or loss of the ballot module. So there is no reason to prevent access to the stores votes by cryptographic signatures. Furthermore the related key management would mean an extra burden for the election staff. Also there is no need for encryption of the votes to prevent reading of the votes. A further disadvantage of encryption is that it makes the ballot module less transparent. The ballot module is the primary source of the votes cast on Election Day.

We therefore place emphasis on the physical security measures for the transport of ballot modules.

Conclusions on Physical and Operational Security

The overall critical dependency of the chosen system, including the supply dependency by the hardware suppliers, on the election management software and the contingent dependency on a limited resource base for the development and maintenance of that software.

In order to deal with the situation of loss of the election management software the election management software is placed under escrow to ensure continuity.
In addition it was offered to DOEHLG to buy the election management software so that it could be under the direct control of DOEHLG.

The specific need for enhanced physical and data security measures to be developed and implemented in the transport of votes and other election data on ballot modules and CD's.

We place emphasis on the physical security measures for the transport of ballot modules for reasons set out before in our comments on Findings on Physical and Operational Security.

The need for the establishment by the Manufactures and the Department of comprehensive electronic registers in respect of the identity, location and movement of all items of electronic voting equipment and the need to introduce appropriate documentary controls on the movement of equipment and data both and between elections.

We note the Commission's finding: *The manual records kept by the Manufacturers in respect of the transportation of such voting equipment are not easily referenced against the location of specific machines in Ireland.*
The register the Commission is asking for is in place and operational in manual form.

We note the Commission's finding: *A communications and documentation trail is kept in respect of the equipment during transportation which gives visibility on progress and on any problems arising while in transit and records are maintained by the Manufacturers to account for the delivery of all equipment in Ireland*.

Conclusion

The physical and operational security aspects of the VM, PRU, BM, the embedded software and the procedures in place at the Manufacturers addressing the physical and operational security aspects with the manufacture and transport are of adequate standard. The findings for the security policy management that require attention are equally important for the current paper bases system.
With the proper procedures in place associated with transport, storage and deployment for use the system is ready for use at elections in Ireland.

Where the testing of the hardware and software shows that no substantial failures have been detected, further work should address the procedural side of the election process and not the testing of the election hardware and software.

Nedap N.V.

Henk Steentjes

Nedap Comments[87] on Part 5

Mr. Alan Murphy Secretary
Commission on Electronic Voting
Floor 4
Setanta Centre
Nassau Street
Dublin 2
Ireland

20h March 2006

Dear Mr. Murphy,

In your letter of February 3rd 2006 you invite us to comment on part 5 of the second report of the Commission. We are happy with this opportunity and request you to publish it as part of the report.

You invited Nedap and Powervote individually. We will comment on the issues that concern the Voting Machine (VM), the Programming/Reading Unit (PRU), the Ballot Module (BM) and its embedded software.

2 years after the work of the CEV started in March 2004, the CEV is to issue its 2nd report. In part 5 of this second report the Commission compares the chosen system against the current paper based system for voting at elections and referenda in terms of secrecy and accuracy.

Part 5 of the second report

The Commission has identified criteria for secrecy and accuracy and other relevant attributes that do not relate to secrecy and accuracy and compared the two systems in regard to these criteria.
Secondly the Commission has identified assessed and compared the potential risks to secrecy and accuracy in both systems.

1. Commission's conclusion on comparative assessment

With regard to the comparative assessment the Commission comes to the following conclusions:

First conclusion of the Commission

- *The chosen system has the potential to be superior to the paper system in many significant respects concerning its accuracy.*

We emphasise that the VM, PRU, BM and the embedded software do not only have this potential, but that they are already superior to the paper system.
In fact this is also the conclusion of the Commission whereas they conclude:

[87] At the request of Nedap, these comments have been reproduced by the Commission in the form they were received, subject only to the deletion of page references as they relate to earlier drafts of the Commission's report. The comments also refer to text contained in earlier drafts that has been revised in the final version of the report.

"*From further examination of the above risks, it is suggested that the risks to accuracy in the chosen system are fewer and of lower magnitude than in the paper system. However this is based on the assumption that the chosen system can be shown to be reliable and behaves as intended in all other respects*".

Taking the above into account, we cannot find any evidence in the second report that show that the paper system is superior in terms of accuracy of the vote capture process, whereas the audits and tests done by the accredited Independent Test Authorities assure the reliability. This reliability is confirmed by the fact that the additional audits and tests carried out in the past two years by the Commission show no failures in the VM, PRU, BM and the embedded software.

Second conclusion of the Commission:

- *The chosen system is unlikely to exceed the standard of secrecy offered by the paper system and, as currently configured; it fails to meet this standard.*

The Commission finds in C.20 that on the important issues of breach of secrecy by collusion or duress, the chosen system is superior because under the paper system it is possible for a third party to have control even in the polling booth over what preferences the voter makes.
In C.22 the Commission finds that under the paper system ballot papers can be marked in a way that it can be identified during the count, thereby breaching the secrecy of the ballot.

The Commission finds in the risk analysis:
"*The risks to secrecy under both systems are low. However, the risks to secrecy under the chosen system at least equal, and in most cases exceed, the risks under the paper system. Two areas of risk are significantly higher in the chosen system*".

The Commission finds the risks to secrecy under both systems low, but we conclude that the possibility of breach of secrecy by collusion and duress under the paper system is significant.

On basis of the arguments given above we conclude that the secrecy offered by the VM, PRU, BM and the embedded software is superior to the secrecy offered by the paper system.

Third conclusion of the Commission:

- *The achievement of the full potential of the chosen system in terms of both secrecy and accuracy depends upon a number of modifications, both major and minor, being made to its present configuration and, more significantly, is heavily reliant on the trustworthiness and reliability of the chosen system being adequately proven.*

As we have shown in our comments mentioned below, the VM, PRU, BM and the embedded software have the necessary qualities and abilities concerning accuracy and secrecy as usability, error detection and prevention, audit facilities and the audits and tests carried out by accredited Independent Test Authorities (ITA's).
Adding extra's may only lead to a more complicated voting process, both for the voter and for the election personnel, unless the benefits of these measures outweigh this.
In our opinion this balance is optimal in the chosen system.

We refer to our comments on

- Usability :
  - Our letter of March 9th 2006 with comments on part 6 enclosure 1 issue 1 page 1.
  - Our letter of February 14th 2006 with comments on part 3 enclosure 1 pages 1, 2 and 3.
- Null, blank votes:
  - Our letter of March 9th 2006 with comments on part 6 page 3 and enclosure 1 issue 13 page 2.
- Accessibility & alternative voting methods for disabled persons
  - Our letter of March 9th 2006 with comments on part 6 page 3 and enclosure 1 issue 3 page 1.
- Audit facilities:
  - Our letter of March 9th 2006 with comments on part 6 page 3 and enclosure 1 issue 100..110 pages 14..16.
- Enhanced measures for the prevention and detection of system failures
  - Our letter of March 9th 2006 with comments on part 6 enclosure 1 issue 30 pages 5 and 6.
- Audits and test carried out by ITA's:
  - Our letter of February 14th 2006 with comments on part 3 pages 2, 4 and 5 and enclosure 1 pages 1, 3 and 4.
  - Our letter of March 9th 2006 with comments on part 6 page 2 and enclosure 1 issue 92 page 13.

Fourth conclusion of the Commission:

- *This proof is currently absent and it is not something that can be easily achieved with the system as currently configured/proposed for use in Ireland.*

As we have commented above, the VM, PRU, BM and the embedded software have been adequately tested by ITA's and the Commission's findings in part 3 found no substantial flaws.
Apparently the Commission wants to ensure her objectivity, but the question remains why the Commission does not in any way take into account the outcome of the investigations and tests carried out by the accredited Independent Test Institutes, the German "Physikalisch Technische Bundesanstalt" and the Dutch TNO.

Our conclusion is that the proof of trustworthiness and reliability of the VM, PRU BM and the embedded software is present in the test reports of these accredited ITA's.

2. In part 5 of the second report also some other essential issues are addressed on which we want to comment.
1) Transparency, Legitimacy and Voter Trust. (C.24)
In C.24 the Commission advocates the use of VVAT as the means to enhance voters trust in the chosen system.
The use of a VVAT does not enhance voters trust as we have indicated in our comments on the first report were we referred to the study of Ted Selker and Jon Goler both from MIT in their Voting Technology Project working paper of April 2004.
The design and thorough tests carried out by Independent Test Authorities combined with the proper procedures ensure the integrity of the chosen system. In addition we favour the use of parallel testing of a random number of VM's to establish voters trust in Ireland.
This view is acknowledged by the recent technical studies on four voting systems by professors at the University of Maryland College Park and Baltimore County campuses of February 2006 (www.elections.state.md.us).

Our detailed comments on transparency, legitimacy and voter trust are given in enclosure 1.

2) Ease of use by Voters (C.25)
The two pilots in 2002 showed that voters found the VM easy to use. Pressing a button is easier than writing.
In the VM the number of the preference is determined by the sequence in which the buttons for the candidates are pressed. This procedure allows people with writing considerations to vote unassisted. This is not the case in the paper system.

More detailed comments on ease of use are given in enclosure 1.

3) General vulnerability to malpractice (C.26)
The possibility within the paper system with regard to secrecy violation by people that have ballot papers available(genuine or bogus ones) who pre-mark ballots and have voters cast these ballots makes the paper system vulnerable for an attack on paper ballots, whereas it is much more difficult to tamper with VM's and BM's in an undetected way.

More detailed comments on malpractice are given in enclosure 1.

4) Summary and analysis of other criteria
The Commission mentions voters trust in the system, ease of use and general integrity as aspects where they find the paper system superior while the strengths of the chosen system concern the important (but less critical in an electoral context) performance issues of speed, scalability and efficiency.

As we have explained above and more in detail in the enclosure 1 to this letter we find that the qualities of the VM, PRU, BM and the embedded software with regard to these issues are higher in comparison to the paper system.

3. Summary
The findings and conclusions of the Commission on accuracy and secrecy together with our comments and the findings of the Commission on the important other criteria mentioned show that in terms of accuracy, secrecy and the other important criteria the qualities of the VM, PRU, BM and the embedded software outweigh the paper system.

These qualities that were aggregated in 30 years of assisting and supplying voting equipment to our customers make the VM, PRU and BM excellently suitable for use in elections as is shown in the Netherlands, Germany and France.

We recommend the use of the system on short notice in a limited number of constituencies in Ireland, since this will present a strong signal to the Irish voters to enhance voters trust, following the thorough investigations carried out by the Commission.

Yours sincerely

Henk Steentjes

Nedap NV
Encl. 1: Detailed comments on analysis and findings of criteria other than secrecy and accuracy.
Encl. 2: Detailed comments on risk analysis.

Enclosure 1. Detailed Comments on the Comparative Assessment as stated in part 5 of the second report of the Commission on Electronic Voting.

Detailed comments on analysis and findings of criteria other than secrecy and accuracy.

Transparency, legitimacy and voters trust (C.24)

The Commission states:

The paper system is also transparent in that, at all stages of the process (except when ballot boxes are in the custody of election officials en route from the polling station to the count centre when the theoretical opportunity for malpractice is at its greatest) the process of casting and counting paper votes is under direct public scrutiny.

Part of the voters trust in the current system is due to the fact that the general public is used to it and one does not think of the possible risks any more.

The process of casting votes is **not** entirely under direct public scrutiny as said by the Commission because the voter marks his ballot in the polling booth in private. There he could swap his ballot paper by a pre marked one and take his own out for the next voter. This is described as “chain voting” by the Commission. This can not be done with a VM.

It is also possible for a voter to take a picture of the marked ballot paper in private environment of the polling booth. It is also possible for voters to take pictures or to film of the ballot as proof for any third party of how he or she has voted. The VM has the advantage that it is still possible for the voter to change the preferences after the picture has been taken.

The problem for the chosen system in establishing trust among sceptics is that it does not transparently translate what voters do in the polling booth into an election result.

Voters enter some preferences into a voting machine, the computers go into action, and an election result is declared.

The main question with regard to voters trust is: Does the VM record the preferences correctly?

The thorough tests by independent accredited Independent Test Authorities (ITA’s), confirmed by test reports guarantee that the hardware and embedded software accurately records the voters preferences. The checks that can be executed at all times on the VM show the correctness of the candidate names and their assignment to the voters panel and the calculated software checksums. The security seals show that no attempts have been made to tamper with the VM or PRU.

The Commission refers to two methods for enhancing further voters trust: Parallel running and a Voter Verifiable Audit Trail (VVAT) (C24).

The Commission states: *Under the chosen system, with no VVAT, there is no independent way of resolving any doubt in an electronic voting result* (C24).

The use of a VVAT does not enhance voters trust as we have indicated in our comments on the first report were we referred to the study of Ted Selker and Jon Goler both from MIT in their Voting Technology Project working paper of April 2004. We favour the use of parallel testing of a random number of VM’s to establish voters trust in Ireland.

This view is acknowledged by the recent technical studies of four voting systems by professors at the University of

Maryland College Park and Baltimore County campuses of February 2006. These reports can be found on the internet: (www.elections.state.md.us).

There are a number of weaknesses associated with VVAT that seldom get attention, but that makes this method unusable for auditing and verifying that the recorded preferences are the preferences cast by the voters.
We will mention some of the weaknesses:

- The voting process becomes more complex. Anything that takes a voters attention away from the selection of preferences and casting the vote will reduce the chance of voting them for the candidates they intended.
- The time required to vote will increase.
- People in general often do not pay attention to receipts, as a consequence voters won't always look at the receipt of the VVAT, so the check by the voter is always far from 100%.
- Variations in formats between the ballot and a verifiable paper receipt make it difficult for people to compare them.
- The VVAT is vulnerable to the fraud it is intended to neutralise: tampered embedded software.
    - If the VM embedded software is tampered and for instance in 1 out of 50 votes the VM prints other preferences than what the voter has chosen and also records this, then there is a big chance that this will not be noticed by the voter. The preferences that are recorded and printed are then not the preferences that the voter has chosen and when the printed receipts are counted by hand the electronically recorded preferences match the paper recordings.
      If the voter notices that the printed preferences do not match is choice he will deselect his preferences and make the choice again and this time the preferences are printed correctly.
      A result manipulated this way will not be detected by the VVAT procedure.
- There could be printed more receipts than that there are voters.
- Problems with printers, like defects or problems with paper jams can cause missing or not readable receipts can compromise the integrity or accuracy of the vote.
- Other disadvantages are the increased complexity of the voting equipment which means an additional burden for the election personnel and additional errors during Election Day in every polling station.

It is clear from the above that the VVAT is not the answer to voters trust.

Parallel election with a random number of VM's, already prepared for the election where the votes are cast under supervision and compared with the result is a far more accurate and transparent way of demonstrating that the VM records preferences accurately than the supposed certainty offered by VVAT.

Furthermore this method does not introduce the above mentioned disadvantages for voters and poll workers in the polling stations.

Ease of use by voters (C.25)

We note the Commission finding: *Most indications from Irish voters who have actually used the voting machine in a real election suggest they found it easy to use when it was deployed in three constituencies on a trial basis in the 2002 Daíl election.* (C25)
It is difficult to see how using the voting machine is easier for any voter than writing preferences on ballot papers; and it is easy to imagine that some elderly or technophobic voters may find using a voting machine more difficult . The paper system is superior in this respect.(C25).

We comment:
The two pilots in 2002 showed that voters found the VM easy to use.
The Commission expects more serious usability issues with multiple polls.
The booth design of the voting machine and the replica ballot interface are a useful and helpful linkage to the paper voting procedure. Instead of writing preferences now the voter presses the button next to the candidate, whose picture is also present on the ballot sheet. In the chosen system the number of the preference is determined by the sequence in which the buttons for the candidates are pressed. This procedure allows people with writing considerations to vote unassisted, which is not the case under the paper system.
In addition to that the VM is prepared for an audio device so that the majority of the visually impaired voters can make use of the VM without assistance.
In the paper based system visually impaired people and individuals with reading considerations normally require assistance, so this would be a significant improvement.
The suggestion that some elderly or technophobic voters may have difficulties in using the VM is not supported by our experience in other European countries.

General vulnerability to malpractice (C.26)
The Commission states: *There is very little possibility for an unauthorised outsider to attack a ballot paper in an undetected way (C26).* The Commission continues: *Attack of the chosen system by an unauthorised outsider is also very difficult though, as reported in Part 3, it is not impossible (C26)* and concludes that *The paper system is thus superior in this respect* (C26)

Here we emphasise the major vulnerability of secrecy violation by people that pre-mark unmarked ballots and have voters cast these ballots in a “chain” voting process.
A possibility to prevent the use of non official ballot papers each official ballot paper should have authentication marks that needs to be checked before the marked ballot paper is cast.

We conclude that the chosen system is superior in respect to general malpractice.

Reliability (C.29)
The Commissions conclusion is*: Overall, however, considering the possibility of undetected failures, the paper system is superior in this respect*. Whereas the current paper system offers the possibility of fraud with pre marked paper ballots in the unsupervised polling booth we think the paper system is not superior.

General integrity
The VM, PRU, BM and the embedded software offer a number of advantages in comparison to the paper system.

- In the paper system the preferences are manually marked on the ballot. Because there is a wide variety in the way voters mark their ballots it is not always clear in the count what the voter’s intentions are. The VM records the preferences on a uniform way that leaves no room for different interpretations during the automated count.
- The possible breaches of secrecy when genuine or bogus paper ballots are pre marked and used persuade voters to “sell” their vote (e.g. in “chain voting” as described by the Commission) do not exist under the chosen system.
- The vulnerabilities to malpractice during storage and during the transport to the polling place and during the transport of the ballots from the polling station to the count centre are higher under the paper system than under the chosen system.

The proprietary hardware and proprietary embedded software of the VM, PRU and BM and the stand alone nature of the VM, the thorough evaluations and testing of the system, the built in facilities to check the integrity of the VM at all times together with the proper procedures before, on and after the Election Day together with the proper procedures ensure the integrity of the VM, PRU and BM.

When the votes are stored in the BM it is possible to do the count more than once, on different PC's and even with different count software or to print the ballots and count by hand. This is an extra way of checking the count process.

With the proper procedures in place the integrity of chosen system is assured and is superior to the paper system.

Enclosure 2. Detailed Comments on the Comparative Assessment: Assessment of Risks, as stated in Appendix 5F of part 5 of the second report of the Commission on Electronic Voting

R.5	Single ballot not recorded.
Description	A ballot is cast by the voter, but not recorded on the ballot module.
Comparison	A small risk in the chosen electronic system, which does not exist in the paper-based system.
Remark	The impact of this risk for EV should be rated as small since the impact of an inadvertently spoiled ballot in R.18 is rated as small for paper voting.

R.28	Voter coercion or bribery
Description	A voter is bribed or intimidated into voting in a particular way.
Comparison	The problem here is verification that the voter has voted as instructed or (in the case of the ballot being taken out of the polling station) has cast the ballot although a fraudster could always cast the ballot him or herself. For a large-scale operation, the risk is slightly greater with an electronic system. For small scale, the situation is comparable in both systems.
Remark	A major disadvantage of the paper system is the vulnerability of malpractice by people in possession of real or bogus paper ballots by which they can influence the voter's choice (see "chain voting" under C20). The probability and impact for the paper system should be rated higher than for the chosen system.

R.29	Substitution of ballots in ballot box/ballot module
Description	A ballot module or modules is switched for a pre-setup module, either at the polling station or at a service centre
Comparison	Doing this is theoretically possible in both cases. Doing it with a paper-based system would require careful observation, suborning several officials and a certain amount of luck. This is a theoretical possibility with the current system, but impractical in reality
Remark	Doing this with an ballot module is very difficult as stated by the Commission in part 3 more than once. Substitution of paper ballots would be easier. The probability under the paper system is therefore higher than under the chosen system.

R.50	Software error in voting machines (wide scale)
Description	A bug in the voting machine software causes it to fail or incorrectly record votes.
Comparison	This is a risk in the chosen electronic system that does not exist in the paper-based system.
Remark	Since the embedded software in the VM has been extensively tested by the accredited German Physikalisch Technische Bundesanstalt, including a source code inspection the probability should be rated as very low instead of moderate.

R.51	Inherent fault in counting process
Description	The votes are recorded and transferred correctly, but the count is wrong.
Comparison	It is virtually certain that there will be errors in a paper-based count. The chances of errors in an electronic count are almost zero and, in any event, the count can be tested using different software if necessary. This is therefore, a higher risk in a paper-based system.
Remark	Regarding the comparison that values the chance of errors in an electronic count as almost zero, the probability under EV should not be rated as moderate but as tiny.

R.59	Alteration of ballots
Description	An attempt to alter the votes on several ballot modules during transportation from polling station to service or count centre.
Comparison	This is a broadly comparable risk with both systems. It would probably be marginally easier to do electronically, given the relative size and manageability of ballot boxes and ballot modules. However, the logistical problems make both frauds improbable.
Remark	See also R.29. Doing this with a ballot module is very difficult as stated by the Commission in part 3 more than once. Substitution of paper ballots would be easier. The probability under the paper system is therefore higher than under the chosen system.

Nedap Comments[88] on Part 6

Mr. Alan Murphy Secretary
Commission on Electronic Voting
Floor 4
Setanta Centre
Nassau Street
Dublin 2
Ireland

9th March 2006

Dear Mr. Murphy,

In your letter of February 3rd you invite us to comment on part 6 of the second report of the Commission. We are happy with this opportunity and request that you publish this letter and enclosure in full as part of the report.

You invited Nedap and Powervote individually and we will comment on issues that concern the Voting Machine (VM), the Programming/Reading Unit (PRU), the Ballot Module (BM) and its embedded software.

2 years after the work of the CEV started in March 2004, the CEV is to issue its 2nd report. In part 6 of this second report the Commission evaluates the chosen system against the Recommendations Rec(2004)11 of the Committee of Ministers of the Council of Europe ("the Recommendation"), agreed in September 2004.

Context of evaluation

The Commission does not consider the Recommendation as the de facto measure because amongst others the Recommendation has no legal status and is non-binding on member states, post-dates to the adoption of the chosen system and has a scope wider than the deployment of the chosen system.

Nevertheless the Commission sees the Recommendation as a valid European agreed point of reference for evaluating the chosen system (resume).

Part 6 of the second report

The Commission has found 86 of the 113 measures of the Recommendation appropriate for evaluation of the chosen system. We found 77 of the 113 measures appropriate for evaluation of the VM, PRU, BM and the embedded software.

The Commission comes to the conclusion that the total chosen system does not comply with 43% of the 86 applicable measures of the Recommendation.
This does not surprise us. The conclusion is mainly based on the supposed shortcomings of the total chosen system as is accounted for by the Commission in part 3 and 4 of the second report.

[88] At the request of Nedap, these comments have been reproduced by the Commission in the form they were received, subject only to the deletion of page references as they relate to earlier drafts of the Commission's report. The comments also refer to text contained in earlier drafts that has been revised in the final version of the report.

However, as the Commission may know, we commented on the VM, PRU, BM and the embedded software and here we disagree with the Commission's findings. We have explained this in our letter of February 14th 2006 on part 3 and in our letter of March 2nd 2006 on part 4 of the second report.

Based on these comments and addressing the issues that relate to the VM, PRU, BM and the embedded software it is logical that we come to another conclusion. We find that the VM, PRU, BM and the embedded software comply with 75 of the 77 applicable measures of the Recommendation.

Area's of non compliance:

Requirement 20: *Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use.*

The way in which e-voting is introduced in Ireland does not contribute to the confidence that voters have in the chosen system. This is due to the appointment of a Commission on Electronic Voting, the subsequent postponement of the planned nationwide introduction of the chosen system in June 2004 and the very long period of testing that followed.

Requirement 66: *Open standards shall be used to ensure that various technical components or services of an e- voting system, possibly derived from a variety of sources, interoperate.*

The VM, PRU and BM hardware and the embedded software are proprietary, so the interface between the system components is not according open standards (requirement 66).

For all clarity now we will address the areas of non-compliance or in need of improvement as mentioned by the Commission in part 6 of the second report.

Need for independent verification, testing and certification of the chosen system

The numerous tests and audits carried out on by Independent Test Authorities (ITA's) on behalf of the Department of Heritage, Environment and Local Government and the test carried out on behalf of the Commission on Electronic Voting have shown that the system accurately records and counts votes and is resistant against environmental threats even beyond specification. We refer to our comments of February 14th 2006 on part 3 of the second report.

Security measures within and around the system

The proprietary hardware and software of the VM, PRU and BM combined with its stand alone nature makes them difficult to tamper with.

Proper procedures enhance the security to an appropriate level. We refer to our comments of March 2nd 2006 on part 4 of the second report.

Procedural controls and staffing requirements

The Department of the Environment Heritage and Local Government should comment on this.

Data security and the use of encryption

Encryption is asked for the BM data including the votes. The election data and the votes are stored onto the BM as non encrypted data. This contributes to the transparency. The necessary key management associated with encryption gives an extra burden to the polling staff, which we do not favour.

When the data is not left unattended we do not see the need for encryption. So also here proper procedures are needed, like checking the authentication of the contents of candidate, lay out and election data in the BM and compare it with the info on the Ballotsheet on the VM. During transport of the BM from the polling station to the count center must be under surveillance, as is the case with Ballot Boxes.
And Ballot Boxes are easier to tamper with, because no special knowledge is required, whereas introducing votes in the BM or bypassing of the VM interface is extremely difficult.
We refer to part 3 of the second report where the Commission states her inability to introduce votes in the BM or to bypass the VM interface number of times (e.g. part 3 second report).
We refer also to our comments of March 2nd 2006 on part 4 of the second report under *use at elections.*

Implementation and facilitation of independent observation and audit

The VM offers a number of audit facilities by which the process of vote registration can be audited.
The hardware and embedded software versions and the checksums can be checked at any time via the display and via the printer. The VM offer the possibility of checking the candidate names as programmed in the BM against the names on the Ballot sheet on the voters panel of the VM. The time marked and signed open and close poll statements show the candidates and layout and the number of votes cast at start of voting (open poll) and the number of votes cast at the end (close poll) where the activation of the printing of the close poll statement locks the BM for further vote storage. The VM directs the voter through the election procedure. The number of voters that have cast votes is shown on the control unit display and is increased every time a new voter casts his preferences.
When the VM malfunctions an error code is displayed to the operator and voter indicating exactly what the problem is. Error codes are also stored in the PRU. Every mode switch (standby mode, voting mode, functions mode) is recorded and time stamped relative to the start of the VM as is the case for every error that occurs.

Accessibility and provision of alternative voting methods for disabled persons

The full face replica of the paper ballot on the voters panel makes the voting process similar to that in the paper voting process. The same facility for voters who need assistance can therefore also be applied.
A tilting table gives greater access to the voting panel for people with disabilities.
Additionally, the VM can be equipped with an audio device so that the majority of the visually impaired voters can make use of the VM without assistance.
In the paper based system visually impaired people and individuals with reading considerations normally require assistance, so this would be a significant improvement.

Allowing null or blank votes

The VM has a built-in abstain facility that was de-activated and unlabeled following our customers decision. It needs to be activated and labelled before it can be used.

Conclusion

We find the VM, PRU and BM in compliance with the Recommendation. This underlines that the VM concept's broad range of qualities can deal with all situations in real elections that are foreseen in the Recommendation. These qualities that were aggregated in 30 years of assisting and supplying voting equipment to our customers make the VM, PRU and BM excellently suitable for use in elections as is shown in the Netherlands, Germany and France.

We recommend the use of the system on short notice in a limited number of constituencies in Ireland, since this will present a strong signal to the Irish voters to enhance voters trust, following the thorough investigations carried out by the

Commission.

Nedap N.V.

Henk Steentjes

Encl.: Detailed comments on Recommendation evaluation.

Comments on the compliance of the VM, PRU, BM and the embedded software to the measures of the Recommendation as stated in Appendix 6B of part 6 of the second report of the Commission on Electronic Voting

We note that the Recommendation states:
E-voting shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means (Appendix A).

1 The voter interface of an e-voting system shall be understandable and easily usable.
Compliance: Good.

Compliance: Very Good.
The voters are purposely not asked for a final conformation of preferences before casting a vote because that can lead to confusion. The full face user interface, that is a replica of the paper ballot, offers the voter a high degree of ''intuitive'' steps to select and review their preferences and to cast their votes. One normally casts the vote only once.

When the VM has a failure, an error message is displayed on the displays of the voters panel and the control unit, thus alarming the operator and the VM halts, so no further action can take place. So the detection of an error and the proper corrective action does not only rely on the voter, but on the more trained operator.

The user interface makes the VM easy to use for voters. That is our experience during the years the system is in use in Europe. Exit surveys held at the pilots during the Dáil elections of 2002 confirm this, also for the people above 65 years.

3 E-voting systems shall be designed, as far as is practicable, to maximise the opportunities that such systems can provide for persons with disabilities.
Compliance: Poor.

Compliance: Good.
The user interface has a full face replica of the ballot paper. After the first 2 pilots the number of rows was reduced from 28 to 14 to allow larger fonts and large LED displays for the preference numbers.
The VM can be placed on a tilt table to allow more disabled people access to the VM. In addition to that the VM is prepared for an audio device so that the majority of the visually impaired voters can make use of the VM without assistance.
In the paper based system visually impaired people and individuals with reading considerations normally require assistance, so this would be a significant improvement.

We feel that in terms of "as far as practicable" the compliance of the VM should be rated as "good" rather than "poor".

5

7

8 Where electronic and non electronic voting channels are used in the same election, there shall be a secure and reliable method to aggregate all votes and calculate the

correct result.
Compliance: Fair.

Compliance: good.
Where two persons work together to enter postal votes in the VM it is likely that the “laboratory conditions” are more met than the “field” conditions. As postal votes are currently counted by hand, ”the double check” when entering postal votes in the VM should lead to less errors. Therefore this complies with the recommendation.

9

10 The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection.
Compliance: Fair.

Compliance: good.
The voter can select his preferences one by one. The user interface with its full face replica of the paper ballot allows the voter to oversee all of his preferences at all times.
The voter is not asked for a final confirmation because this can lead to votes not cast. Our experience in other countries showed that a lot of people do not press the cast vote button twice. Therefore this complies with the recommendation.

11

12

13 The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example by casting a blank vote.
Compliance: Fail.

Compliance: Good.
The VM allows the voters not to press the cast vote button. The VM is then deactivated by the poll staff and the VM stores this deactivation. In multiple elections the null votes are recorded in the BM.
The requirement is met.

The VM has a built-in abstain facility that was de-activated and unlabeled following our customers decision. It needs to be activated and labelled before it can be used.

14

15 The e-voting system shall prevent the changing of a vote once that vote has been cast.
Compliance: Poor.

Compliance: Excellent.
The Commission states (Appendix 6B no 15): *It is impossible for a voter to change a vote once it has been cast and*

extremely difficult for anyone else to change a vote while it is in the ballot module. The requirement is met.

16

17

18

19

20 Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use. Compliance: Fair.

Compliance of the introduction of e-voting in Ireland: fail
Here the Recommendations oblige the member states to ensure that voters understand and have confidence in the system. As the Commission states (Appendix 6B no 20): *a high level of information, education and assistance was provided to voters in the three constituencies where e-voting was used on a pilot basis in 2002. Similar measures were planned for the nation-wide deployment of the system in 2004*.
So the first part of this requirement is met.

The Commission continues (Appendix 6B no 20): *However the doubts raised about the system which lead to the establishment of an independent Commission, the conclusions of the Commission's interim and first reports and the subsequent non-use of the system in 2004 have diminished public confidence in the system to a level that will be extremely difficult to overcome*

The way in which e-voting is introduced does not contribute to the confidence that voters have in the chosen system.

First a system is chosen that has a proven record and subsequently it is adapted to the specific Irish Election conditions. Then it is tested and pilots are run. Adaptations are made according the findings and the system is tested again by DOEHLG and ITA's against the agreed specifications. Then just before the intended use in the European Elections of June 2004 a Commission is installed to investigate if the chosen system is trustworthy and the deployment of the chosen system is postponed.

Now 2 years after the Commission started its work the Commission did not find substantial flaws. The system accurately records and counts votes and with the right procedures in place the secrecy is guaranteed.
But new standards are sought and after two years of investigation the conclusion of the Commission is that still more testing is needed.
This way of introducing the e-voting system in Ireland undermines the confidence of voters in the system. Whereas technology is trusted in supporting nearly all of our activities in daily life we do not understand that a system that is robust and has been tested for years, that is easy to understand and easy to use, cannot assist voters in electing the people who they want as their representatives in local and national government.
Our conclusion on this requirement is: The requirement is not met.

22

23 *Any observer, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishments of the results.*
Compliance: Poor.

Compliance: Good.
There are facilities available for observers**.**
The VM offers a number of audit facilities by which the process of vote registration can be audited.
The hardware and embedded software versions and the checksums can be checked at any time via the display and via the printer. The VM offer the possibility of checking the candidate names as programmed in the BM against the names on the Ballotsheet on the voters panel of the VM. The time marked open and close poll statements show the candidates and layout and the number of votes cast at start of voting (open poll) and the number of votes cast at the end (close poll) where the activation of the printing of the close poll statement locks the BM for further vote storage. The VM directs the voter through the election procedure. The number of voters that have cast votes is shown on the control unit display and is increased every time a new voter casts his preferences.
When the VM malfunctions an error code is displayed to the operator and voter indicating exactly what the problem is. Every mode switch (standby mode, voting mode, functions mode) is recorded and time stamped relative to the start of the VM as is the case for every error that occurs. The requirement is met.

24 The components of the e-voting system shall be disclosed, at least to competent electoral authorities, as required for verification and certification purposes.
Compliance: Fair.

Compliance: Excellent.
All the design issues including the embedded source code and the worst case calculations of the electronic hardware were made available to accredited Independent test Authorities (ITA's) and to the Commission on Electronic Voting. The VM, PRU, BM and the embedded software were intensively audited and tested including a source code inspection by the PTB. Numerous environmental tests were carried out. Of all these tests are reports available. The requirement is met.

25 Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular, after any changes have been made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is working correctly and that all security measures have been taken.
Compliance: Fail.

Compliance: Excellent.
See 24. In the "Requirements for voting machines for use at elections in Ireland DVREC-2" of March 5, 2003 it is foreseen that a periodic inspection shall take place. The requirement is met.

26 There shall be the possibility of a recount. Other features of the e-voting system that may influence the correctness of the results shall be verifiable.
Compliance: Poor.

Compliance: Very good.

The votes in the BM can be printed if legal force is applied. The ballot papers can be counted as the mix can be restored because the ballots of the mix are known in the count software.
The voting machines integrity can be tested in parallel voting sessions or a from a number of randomly chosen VM's the embedded software can be compared with the code that is released in the test report. The requirement is met.

27

28 *The member state's authorities shall ensure the reliability and security of the e-voting system.*
Compliance: Poor.

Compliance: Good.
The reliability and security of the VM, PRU, BM and its embedded software is very good as can be seen in the test reports of the ITA's that have tested the VM, PRU and BM according the specifications as agreed to with DOEHLG and also no errors were found during the two years of testing by the Commission.

The Commission confirms the reliability and security in part 3 of the second report:
The main hardware components of the system, namely the voting machine, the programming/reading unit and the ballot module are of good quality and design. They are robust against failure and are generally well suited to their purpose. Further investigation, refinement, testing and independent certification of these components would however be necessary before they could be confidently recommended for use at elections in Ireland" (part 3).

"The embedded C code software within the voting machine and programming/reading unit is of an adequate standard and, while it is not of mission critical standard, there is evidence to suggest that it has been developed according a recognisable structured design process which is broadly in accordance with industry best practice. (part 3).
Therefore the requirement is met.

29 *All possible steps shall be taken to avoid the possibility of fraud or unauthorised intervention affecting the system during the whole voting process.*
Compliance: Fail.

Compliance: Good
The proprietary hardware and embedded software and the stand alone nature of the VM and PRU and BM makes it difficult for anyone to tamper with.
The Commission's statement in part 3 underlines this:
"*the Commission was unable to exercise the ballot module and other downstream components of the system using large numbers of known votes introduced authentically using a test harness, either to bypass the voting machine interface or to introduce them directly onto the ballot module itself. Although this was a limitation on the Commission's proposed work, it also represents a significant strength of the system. It shows the degree of difficulty presented to anyone seeking maliciously to introduce large numbers of votes to the system at an election, via either a voting machine interface or a ballot module*".
The requirement is met.

30 *The e-voting system shall contain measures to preserve the availability of its service during the e-voting process. It*

shall resist, in particular, malfunction, breakdowns or denial of service attacks.
Compliance: Fair.

Compliance: Very good.
We note the Commission's statement on this (Appendix 6B no 30): *The hardware and software used for voting and for transport of votes to read-in centres are generally robust against malfunction, breakdown and denial of service.*
Therefore the compliance with the Recommendation should be rated as good.

31 Before any e-election or e–referendum takes place, the competent electoral authority shall satisfy itself that the e-voting system is genuine and operates correctly.
Compliance: Fail.

Compliance: Good.
All EMS system components were independently tested for compliance against the specifications on behalf of DOEHLG. The VM, PRU and BM hardware and embedded software were tested by the German Independent Test Authority "Physikalisch Technische Bundesanstalt" (PTB).
Important to mention is that the PTB did the static analysis on the VM and PRU internal embedded C code software and did the manual source code inspection asked for in part 3 of the Commission's second report by which potential run-time errors were discharged.
The environmental tests including electromagnetic compatibility, electrical tests, temperature tests, shock & vibration tests and drip water tests were carried out by the accredited Dutch TNO. The safety tests were carried out by the accredited Dutch KEMA.

The software and hardware configuration of the VM and PRU can be reported through the software and hardware itself. The embedded software calculates its own checksums at start-up and these are displayed as well as the hardware configuration. This can be checked. The assignment of the candidates to the voters panel and their names can be checked against the ballot paper on the voters panel and these are printed in the time marked and signed open poll and close poll statements at the beginning and the end of the poll. So the requirement is met.

32 Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. Critical technical activities shall be carried out by teams of at least two people. The composition of the team shall be regularly changed. As far as possible, such activities shall be carried out outside election periods.
Compliance: Poor.

Compliance: Good.
We note the Commission's statement on this(Appendix 6B no 32): *While teams of two are used at the counting stage, the voting machine is currently proposed to be operated by one person only.*
That is correct. But the Recommendation says*: Critical technical activities shall be carried out by teams of at least two persons.* The operation of the VM is an operational activity and not a critical technical activity.
The maintenance and service functions of the system are critical functions of the VM. Personnel of the manufactures and suppliers are foreseen to help the election personnel on the help desk. It is up to the electoral authority to appoint and train election staff to execute the maintenance and service functions. It is a matter of proper procedures.
So the requirement is met.

33 While an electronic ballot box is open, any authorised intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report, be monitored by representatives of the competent electoral authority and election observers.
Compliance: Poor.

Compliance: Good.
The operation of the VM, that is activating the VM for a voter or deactivating it when someone did not press the Cast Vote button is not an intervention but a normal operational activity. This can be done by one person.
Interventions like opening (open poll statement) and closing (close poll statement and back-up of BM) or handling when there is an error in the VM is normally foreseen to be done by more than one person. So the requirement is met.

34 The e-voting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.
Compliance: Poor.

Compliance: Good.
We note the Commission's statement on this i(Appendix 6B no 34): *the controls within the voting machine and ballot module to maintain availability and integrity of the votes once cast are good.*

However the measures to maintain the confidentiality are less than would be desirable as votes stored on the ballot are not encrypted or cryptographically signed. Here we comment:

In part 4 of the second report the Commission states: *The transport of the ballot module from the polling station to the read-in and count centre is the most sensitive stage in the entire life-cycle process of the chosen system. There is a low risk associated with the main theoretical threat of the substitution of a ballot module that has been programmed with bogus votes by a person with access to the election management software and a programming/reading unit. However there are also the threats of accidental or deliberate damage, destruction or loss of the ballot module which, notwithstanding the existence of a backup ballot module, can have an impact on confidence in the electronic voting syste*m (Part 4).

The main theoretical threat of substitution of a ballot module with one that has been programmed with bogus votes is also confirmed several times in Part 3 of the second report. We refer to the finding of the Commission in Part 3: *the Commission was unable to exercise the ballot module and other downstream components of the system using large numbers of known votes introduced authentically using a test harness, either to bypass the voting machine interface or to introduce then directly onto the ballot module itself. Although this was a limitation on the Commission's proposed work, it also represents a significant strength of the system. It shows the degree of difficulty presented to anyone seeking maliciously to introduce large number of votes to the system at an election, via either a voting machine interface or a ballot module.*

The risk of substitution of a ballot module with one that has been programmed with bogus votes is mainly theoretical and is even further mitigated by the physical security measures that mitigate the risk of accidental or deliberate damage, destruction or loss of the BM.

A disadvantage of encryption or cryptographically signing is that it makes the ballot module less transparent. Remember that the BM is the primary source of the votes cast on Election Day.
Furthermore the related key management would mean an extra burden for the election staff.

Since there is no reason to prevent access to the stores votes by encryption or to apply cryptographically signing, we place emphasis on the physical security measures for the transport of BM's.
The requirement is met.

35

38

47

48

52

53

54

55

56

58 In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such.
Compliance: unknown

Compliance: Good.
Each vote consists of 4 vote copies that are separately stored in the BM and have an error detection mechanism. 3 out of the 4 copies of a specific vote must be defective or 2 by 2 unequal before this vote is invalid. The affected vote (correct and defective copies) remain in the BM. Only valid votes are counted. The change that a vote is invalid is extremely small due to the redundancy.

59 The e-voting system shall be auditable.
Compliance: Poor.

Compliance: Good.
The VM offers a number of audit facilities by which the process of vote registration can be audited.
The hardware and embedded software versions and the checksums can be checked at any time via the display and via the printer. The VM offer the possibility of checking the candidate names as programmed in the BM against the names on the Ballot sheet on the voters panel of the VM. The time marked and signed open and close poll statements show the

candidates and layout and the number of votes cast at start of voting (open poll) and the number of votes cast at the end (close poll) where the activation of the printing of the close poll statement locks the BM for further vote storage. The VM directs the voter through the election procedure. The number of voters that have cast votes is shown on the control unit display and is increased every time a new voter casts his preferences.
When the VM malfunctions an error code is displayed to the operator and voter indicating exactly what the problem is. Error codes are also stored in the PRU. Every mode switch (standby mode, voting mode, functions mode) is recorded and time stamped relatively to the start-up of the VM as is the case for every error that occurs.
The requirement is met.

61 Measures shall be taken to ensure that the relevant software and services can be used by all voters, and if necessary, provide access to alternative ways of voting.
Compliance: Poor.

Compliance: Good.
See 3.

62 Users shall be involved in the design of e-voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.
Compliance: Fail.

DOEHLG has been looking for an e-voting system that had a proven track record. The chosen system is the result of 30 years of experience with the infrequent and somewhat unpredictable nature of elections. We have learned from election personnel and voters that the best practice is to keep the election process as simple as possible. Over the years the effects of user involvement is clearly seen. Ease of use in combination with transparency has always been the guiding principle in the development of voting systems.
We have stayed as close as possible to the user interface that the voters are used to in paper voting systems, the VM has a full face replica of the ballot paper.

When DOEHLG had chosen for the Nedap Powervote concept the VM was adapted to the Irish election system. Two pilots were held and after evaluation adaptations to the VM were made accordingly, including to the findings of voters and poll staff.
E.g. the number of rows was reduced from 28 to 14 to allow larger fonts and large LED displays for the preference numbers.
The requirement is met.

63 Users shall be supplied, whenever required and possible, with additional facilities, such as special interfaces or other equivalent resources, such as personal assistance. User facilities shall comply as much as possible with the guidelines set out in the Web Accessibility Initiative (WAI).
Compliance: Poor.

Compliance: Good.
The user interface is a full face replica of the paper ballot which makes the voting process easy to understand. A tilting table is provided for easier access to the VM for people with disabilities. The voters can have personal assistance as

they have in paper based system.
Additionally, the VM can be equipped with an audio device so that the majority of the visually impaired voters can make use of the VM without assistance.
In the paper based system visually impaired people and individuals with reading considerations normally require assistance, so this would be a significant improvement.
The requirement is met.

64 Consideration shall be given, when developing new products, to their compatibility with existing ones, including those using technologies designed to help people with disabilities.
Compliance: Fail.

Compliance: Good.
See 63.

65

66 Open standards shall be used to ensure that various technical components or services of an e-voting system, possibly derived from a variety of sources, interoperate.
Compliance: Fail.

Compliance: Fail.
No open standards are used but proprietary hardware and software. The basic components of the system, the VM, PRU and BM on the one hand and the Integrated Election Software are in use for many years in the Netherlands and Germany and the interoperability of the system components is very good

69 The competent electoral authorities shall publish a list of the software used in an e-election or e-referendum. Member states may exclude from this list data protection software for security reasons. At the very least, it shall indicate the used software, the versions, its date of installation and a brief description. A procedure shall be established for regularly installing updated versions and corrections of the relevant protection software. It shall be possible to check the state of the protection of the voting equipment at any time.
Compliance: Fail.

Compliance: Very good.
We note the Commission's statement on this (Appendix 6B no 69): *Although these requirements refer more to integrated election systems operating over networks based on communication standards of hardware and software, they also illustrate the limitations imposed by the proprietary nature of the chosen system.*
We comment: The embedded software and hardware versions and the embedded software checksums of the VM and PRU are published in the test reports. On every VM the hardware and embedded software versions and the checksums can be checked at any time via the display and via the printer. When the embedded software should be updated, it would be tested again by an ITA and published in the test report.
Therefore the requirement is met.

70

71

76 Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the competent electoral authorities, who will take the necessary steps to mitigate the effects of the incident. The level of incident which shall be reported shall be specified in advance by the electoral authorities.
Compliance: Fair.

Compliance: Good.
We note the Commission's statement on this (Appendix 6B no 76): *The arrangements for intervention and reporting by election officials and for the provision of technical assistance in the event of irregular incidents concerning the hardware and software during voting are very good. However, the detection of many potential malfunctions of the voting machine falls in practice to the voter as the main user of the machine and may thus remain undetected by the operator.*
We comment: The VM constantly checks itself and in case of malfunction a specific error code indicating the specific error is displayed on the displays of the voters panel and the control unit, thus alarming the operator and the VM halts, so no further action can take place. So the detection of an error and the proper corrective action does not only rely on the voter, but on the more trained operator.
The requirement is met.

77

79 The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available.
Compliance: Poor.

Compliance: Good.
At start-up the VM calculates the checksums of its embedded software, checks the election data, candidate names, ballot lay-out and the votes in the BM and checks the hardware components. The software checksums, the hardware and software versions can be verified by poll staff at all times. After start-up of the VM the checks on the election data, candidate names, ballot lay-out, the votes in the BM and the hardware components are constantly repeated. The open poll and close poll statements are printed, checked and time stamped and signed by poll staff.
The requirement is met.

80 The e-voting system shall restrict access to its services, depending on the user identity or the user role, to those services explicitly assigned to this user or role. User authentication shall be effective before any action can be carried out.
Compliance: Poor.

Compliance: Good.
The VM has keys and locks for physical access. In the chosen system user authentication of operators and voters is a manual process. With the proper procedures in place restricted access depending on the user identity or the user role is guaranteed. Therefore the requirement is met.

83 E-voting systems shall generate reliable and sufficient detailed observation data so that election observation can be carried out. The time at which an event generated observation data shall be reliable determinable. The authenticity,

availability and integrity of the data shall be maintained.
Compliance: Poor.

Compliance: Good.
The VM offers a number of audit facilities by which the process of vote registration can be audited.
The hardware and embedded software versions and the checksums can be checked at any time via the display and via the printer. The VM offer the possibility of checking the candidate names as programmed in the BM against the names on the Ballot sheet on the voters panel of the VM. The time marked and signed open and close poll statements show the candidates and layout and the number of votes cast at start of voting (open poll) and the number of votes cast at the end (close poll) where the activation of the printing of the close poll statement locks the BM for further vote storage. The VM directs the voter through the election procedure. The number of voters that have cast votes is shown on the control unit display and is increased every time a new voter casts his preferences.
When the VM malfunctions an error code is displayed to the operator and voter indicating exactly what the problem is. Error codes are also stored in the PRU. Every mode switch (standby mode, voting mode, functions mode) is recorded and time stamped relative to the start of the VM as is the case for every error that occurs.
There is no time clock in the system because this could threaten the secrecy of the votes.
The requirement is met.

84 *The e-voting system shall maintain reliable synchronised time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observation data, as well as for maintaining the time limits for registration, nomination, voting or counting.*
Compliance: Fair.

Compliance: Good.
Besides errors also mode switch events (standby mode, voting mode, functions mode) are time stamped relative to the start of the VM. There is no time clock in the system because this could threaten the secrecy of the votes.
The requirement is met.

89 *The integrity of data communicated from the pre-voting stage, (e.g. voter's registers and lists of candidates) shall be maintained. Data-origin authentication shall be carried out.*
Compliance: Poor.

Compliance: Good.
The VM offers the possibility of printing the open poll and close poll statements. These are time marked and signed. Here the candidate names, the lay out of the candidates on the voters panel, the software checksums and software and hardware versions are shown. Every time the VM is released for a new voter the integrity of the candidate names and the lay out of the candidates on the voters panel present in the BM, is checked for integrity by the VM.
The candidate names and the lay-out of the candidates on the voters panel can be checked in functions mode at all times. Therefore the requirement is met.

91 *The fact that a vote has been cast within the prescribed time limits shall be ascertainable.*
Compliance: Poor.

Compliance: Good.

There is no time marked of the votes as this may infringe the secrecy of the votes. The time marked and signed open poll statement witnesses that before open poll there were no votes cast (number of voters is on open poll statement) and the time stamped close poll statement witnesses that no votes were cast after that time (after close poll statement voting is blocked by the BM). So the requirement is met.

92 *Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that could modify the vote.*
Compliance: Fair.

Compliance: Very good.
We note the Commission's statement on this(Appendix 6B no 92): *Votes could be modified on the ballot module but with some considerable difficulty of access.* We comment: In Part 3 of the second report the Commissions states: *the Commission was unable to exercise the ballot module and other downstream components of the system using large numbers of known votes introduced authentically using a test harness, either to bypass the voting machine interface or to introduce then directly onto the ballot module itself. Although this was a limitation on the Commission's proposed work, it also represents a significant strength of the system. It shows the degree of difficulty presented to anyone seeking maliciously to introduce large number of votes to the system at an election, via either a voting machine interface or a ballot module.*

We note the Commission's statement(Appendix 6B no 92): *Further investigation is required to establish the trustworthiness of the voting machine software that is responsible for handing the storage of votes on the ballot module.* We comment: **The embedded software is intensively tested by the German Physikalisch Technische Bundesanstalt, including a full source code review and source code inspection. The Commission has reviewed the software for 2 years now and found no substantial flaws. Our conclusion here is that there is no need for further investigation and it would only undermine the trustworthiness in the eyes of the public.**
The requirement is met.

93

95

96

97 *The integrity of data communicated during the voting stage (e.g. votes, voter's registers, list of candidates) shall be maintained. Data-origin authentication shall be carried out.*
Compliance: Poor.

Compliance: Good.
See 89 for candidate info and 92 for data integrity of the BM.
The requirement is met.

98

99

100 The audit system shall be designed and implemented as part of the e-voting system. Audit facilities shall be present on different levels of the system: logical, technical and application.
Compliance: Fail.

Compliance: Good.
The VM offers a number of audit facilities by which the process of vote registration can be audited.
The hardware and embedded software versions and the checksums can be checked at any time via the display and via the printer. The VM offer the possibility of checking the candidate names as programmed in the BM against the names on the Ballot sheet on the voters panel of the VM. The time marked and signed open and close poll statements show the candidates and layout and the number of votes cast at start of voting (open poll) and the number of votes cast at the end (close poll) where the activation of the printing of the close poll statement locks the BM for further vote storage. The VM directs the voter through the election procedure. The number of voters that have cast votes is shown on the control unit display and is increased every time a new voter casts his preferences.
When the VM malfunctions an error code is displayed to the operator and voter indicating exactly what the problem is. Error codes are also stored in the PRU. Every mode switch (standby mode, voting mode, functions mode) is recorded and time stamped relative to the start of the VM as is the case for every error that occurs.
The requirement is met.

101 End-to-end auditing of an e-voting-system shall include recording, providing monitoring facilities and providing verification facilities. Audit systems with the features set out in No's 102 to 110 below shall therefore be used to meet these requirements.
Compliance: Fail.

Compliance: Good.
See 102 to 110

102 The audit system shall be open and comprehensive, and actively report on potential issues and threats.
Compliance: Fail.

Compliance: Good.
See 100.

103 The audit system shall record times, events and actions, including:
- *a. all voting-related information, including the number of eligible voters, the number of votes cast, the number of invalid votes, the counts and recounts, etc,;*
- *b. any attacks on the operation of the e-voting system and its communications infrastructure;*
- *c. system failures, malfunctions and other threats to the system.*

Compliance: Fail.

Compliance: good.
The VM and PRU record the events and actions under a. b. and c.
The number of voters that have cast votes on the VM is shown on the control unit display and is increased every time a new voters casts his preferences.

When the VM malfunctions an error code is displayed to operator and voter on the voters and control unit displays indicating exactly what the problem is. Error codes are also stored in the PRU. Every mode switch (standby mode, voting mode, functions mode) is time stamped relative to the start of the VM and recorded as is every error that occurs.
The requirement is met.

104 The audit system shall provide the ability to oversee the election or referendum and to verify that the results ands procedures are in accordance with the applicable legal provisions.
Compliance: Fail.

Compliance: Good.
With the presence of seals and locks, the ballot paper on the VM voters panel, the open poll statement, the number of voters that have cast votes that is shown on the control unit display, the error codes, the close polls statements, the hardware and software version numbers, software checksums and the time stamped error and event logging provide an oversight of the election or referendum.
The requirement is met.

105 Disclosure of the audit information to unauthorised persons shall be prevented.
Compliance: N/A

Compliance: Good.
The time stamped errors and events that are recorded can only be shown in a special mode.
The requirement is met.

106 The audit system shall maintain voter anonymity at all times.
Compliance: N/A

Compliance: Good.
See 16 to 19 and 105. The requirement is met.

107 The audit system shall provide the ability to cross-check and verify the correct operation of the e-voting system and the accuracy of the result, to detect voter fraud and to prove that all counted votes are authentic and that all votes have been counted.
Compliance: Fail.

Compliance: Good.
The actual number of voters for each election are constantly displayed on the control panel for the operator and these are printed in the close poll statement. The proprietary hardware and software of the VM, PRU and BM, their stand alone nature and the physical seals and locks makes it difficult to tamper. The in depth evaluation and testing by accredited Independent Test Authorities is proof that the VM, PRU and BM accurately record voters preferences. The final proof that the votes cast are the votes counted is to use a random number of VM's in a parallel election with the input of known preferences.
The requirement is met.

108 The audit system shall provide the ability to verify that an e-election or e-referendum has complied with the

applicable legal provisions, the aim being to verify that the results are an accurate representation of the authentic votes.
Compliance: Fail.

Compliance: Good.
See 107.

109 The audit system shall be protected against attacks which may corrupt, alter or lose records in the audit system.
Compliance: Fail.

Compliance: Very good.
The Commission states (Appendix 6B no 109): *The protection against alternation or loss of the limited audit data generated by the voting process (vote tallies at open and close of poll and error logs) are very good but their value is limited.* As we have pointed out several times (no 23, 59, 83, 100) there is more audit data then described here by the Commission.
The VM offers a number of audit facilities by which the process of vote registration can be audited.
The hardware and embedded software versions and the checksums can be checked at any time via the display and via the printer. The VM offer the possibility of checking the candidate names as programmed in the BM against the names on the Ballot sheet on the voters panel of the VM. The time marked and signed open and close poll statements show the candidates and layout and the number of votes cast at start of voting (open poll) and the number of votes cast at the end (close poll) where the activation of the printing of the close poll statement locks the BM for further vote storage. The VM directs the voter through the election procedure. The number of voters that have cast votes is shown on the control unit display and is increased every time a new voter casts his preferences.
When the VM malfunctions an error code is displayed to the operator and voter indicating exactly what the problem is. Error codes are also stored in the PRU. Every mode switch (standby mode, voting mode, functions mode) is recorded and time stamped relative to the start of the VM as is the case for every error that occurs.
There must be proper procedures in place to protect the paper audit material.
The requirement is met.

111 Member states shall introduce certification processes that allow for any ICT component to be tested and certified as being in conformity with the technical requirements described in this recommendation.
Compliance: Fail.

Compliance: Good.
The Department of the Environment, Heritage and Local Government introduced its own certification process for testing of the VM, PRU, the BM and the embedded software.
The VM, PRU and BM's hardware and software were tested by the German accredited Independent Test Authority "Physikalisch Technische Bundesanstalt" (PTB), including a full source code review and source code inspection.
The environmental tests including Electromagnetic Compatibility, electrical tests, temperature tests, shock & vibration tests and drip water tests were carried out by the Dutch accredited Independent Test Authority TNO. The safety tests were carried out by the Dutch accredited Independent Test Authority KEMA.
In Germany the PTB is appointed by the federal government to test the compliance of Voting Machines with the technical requirements.
The requirement is met.

112 In order to enhance international co-operation and avoid duplication of work, member states shall consider whether their respective agencies shall join, if they have not done so already, relevant international mutual recognition arrangements such as the European Co-operation for Accreditation (EA), the International Laboratory Accreditation Co-operation (ILAC), the International Accreditation Forum (IAF) and other bodies of similar nature.
Compliance: excellent.

Compliance: Excellent.
The Commission should not start all over again, but should build on what has already been done by the Department of the Environment, Heritage and Local Government.
The Department has sought accredited Independent Test Authorities with experience in testing e-voting systems.
In Germany the PTB is appointed by the federal government to test the compliance of Voting Machines with the technical requirements.
That is why they asked the the German accredited Independent Test Authority "Physikalisch Technische Bundesanstalt" (PTB), to evaluated and test the The VM, PRU and BM's hardware and software, including a full source code review and source code inspection.
The environmental tests including Electromagnetic Compatibility, electrical tests, temperature tests, shock & vibration tests and drip water tests were carried out by the Dutch accredited Independent Test Authority TNO. The safety tests were carried out by the Dutch accredited Independent Test Authority KEMA. Both have experience is these tests for Voting Machines.
The requirement is met.

Response by Commission to Nedap Comments

Mr. Henk Steentjes
Head of Development
Nedap NV
Parallelweg 2g
105 NL-7141 DC
Groenlo
The Netherlands

Second Report of the Commission

Dear Mr. Steentjes

I enclose for your information the Commission's response to your comments on of the Commission's draft report as contained in your letters to me of 14 February, 2 March, 9 March, 20 March, 11 April and 9 June.

The Commission has noted that your comments relate only to the voting machine, the programming-reading unit, the ballot module and the embedded C code software.

I confirm that your comments will be included in the report when it is presented, together with the Commission's enclosed response.

I also acknowledge your request that your comments be included in their original form, notwithstanding that they may refer to parts of the Commission's report that have subsequently been revised. However the page and paragraph references to earlier drafts of the report have been removed as they do not refer correctly to the final version.

The Commission has reviewed its report in light of your comments generally and a number of changes have been made on this basis.

I would like to take this opportunity to thank you and your colleagues for your cooperation with the Commission in its work.

Yours sincerely

_____
Alan Murphy
Secretary to the Commission

29 June, 2006

Second Report of the Commission on Electronic Voting

Response by Commission (CEV) to Nedap Comments on Versions 3 and 6

Part 3 (Nedap letter of 14 February)

Issue 1: Testing and Analysis Work on Embedded C code Previously Carried out by PTB

Nedap Comment: PTB did the static analysis on the VM and PRU embedded C-code software. They performed automated analysis and performed a manual source code inspection asked for in the Commission's report by which potential run-time errors were discharged. Owing to the documentation of each individual test scenario in test protocols, which are archived at the PTB, each of the tests performed is repeatable. We do not see why this has to be repeated again.

CEV Response: It was the Commission's preferred choice to have its own independent analysis and testing of the code carried out rather than reviewing or relying on work carried out previously by PTB for either Nedap or the Department.

Issue 2: Adequacy of Specifications

Nedap Comment: … the Commission is seeking new standards and specifications to judge the chosen system. We do not see an analysis of the agreed specifications and we do not see a clear definition of amended specifications. If the agreed specifications of 2003 are not adequate to support elections in a trustworthy way we invite the Commission to specify why not and what amendments should be made.

CEV Response: The Commission does not find or conclude, as suggested above, that the agreed specifications of 2003 are not adequate to support elections in a trustworthy way and has clarified in section 2.7 of Part 2 that many of the non-technical requirements that formed the basis of the adoption and procurement of the system in fact lie beyond the scope of its work.

However, and as indicated in section 2.3 of Part 2, the Commission did seek to review the technical requirements and specifications for the system and found them insufficient to support the formal methods approach it had originally intended (but that less formal analysis and testing could still be carried out to assess the system further). The Commission's work proceeded on this basis.

Issue 3: Requirement for Further Investigation, Refinement and Independent Certification

Nedap Comment: Further investigation, refinement and independent certification is only meaningful if the Commission defines why the existing specifications are not sufficient and what amendments should be made.

CEV Response: The Commission's response on specifications is set out at Issue 2 above. As regards further investigation, refinement and certification of the system, the Commission's earlier

reports reviewed the previous testing of the system and concluded that it was incomplete in ways and limited in other ways. The Commission has indicated that further analysis and testing would also be required to address a number of specific issues raised by its second report. The Commission's work has also highlighted the need for certain modifications and additions to the system and it would be preferable that these should be carried out first. Finally, the Commission has recommended that the additional analysis and testing work should be carried out, and the whole system verified and assured, by a single independent body.

Issue 4: Standards Applied by the Commission

Nedap Comment: We would like to know from the Commission what the standards are that the VM was tested against.

CEV Response: The Relevant EMC Standards have been specified in footnotes to Part 3 of the report.

Issue 5: Software Quality Management Plan not Supplied

Nedap Comment: We did supply to QinetiQ the project overview of the development of the ESI2 voting machine embedded software with details on the software conventions.

CEV Response: This matter has now been clarified.

Issue 6: Correlation between Software/Hardware and Documentation

Nedap Comment: We would like to know from the Commission where the documentation is not in correspondence to the source code.

CEV Response: This matter has now been clarified.

Issue 7: Adequacy of Design, Development and Documentation Processes

Nedap Comment: We are astonished …

CEV Response: This and other comments represented the Commission's overall findings concerning the software and other components and features of the system as a whole, i.e. including in this case both the C-code and the Delphi code software. This reference has been deleted from the report while the Commission's findings on each individual hardware and software component remain in sections 3.2 and 3.3.

Issue 8: Two Years of Testing

Nedap Comment: After reading Part 3 we must conclude that in two years of evaluation and additional testing the Commission did not find any substantial flaws in the VM, PRU and BM hardware and embedded software of the chosen system.

CEV Response: The Commission has clarified in section 2.1 of Part 2 that its role was not to test the system but to form an independent view of its secrecy and accuracy, including as compared with the paper system. The Commission's role and work have thus been more broadly based than merely testing the system for flaws and, while some additional testing has been carried out in accordance with the Commission's terms of reference, it is incorrect to suggest that the Commission has spent two years testing the system and has come up with nothing substantial as a result.

Part 5 and Appendix 5 (Nedap letter of 20 March)

Issues that are not strictly related to secrecy and accuracy have been moved to a new Appendix 5A to clarify that, while they have been included for completeness, they do not form part of the Commission's comparative assessment. Some comparators of lesser significance have been deleted.

Part 6 and **Appendix 6** (Nedap letter of 9 March)

CEV Response (General): It should be noted that while individual Nedap components may meet or exceed certain requirements of the recommendation, the Commission's evaluation relates to the overall compliance with the recommendation of the Irish implementation of e-voting, that is, the chosen system as a whole (Nedap and Powervote components) as well as the procedures for its deployment. Thus the evaluation in each case takes account of the combined strengths and weaknesses of these different components and procedures.

Issue 9: Audit

Nedap Comment: As we have pointed out several times (no 23, 59, 83, 100) there is more audit data than described here by the Commission.

CEV Response: It is noted that audit information is recorded by both the voting equipment and the counting equipment that would make it possible to monitor and verify that an election had been properly conducted in accordance with law (and this has been acknowledged in the evaluations on measures 103 and 104). However, the system does not currently appear to provide audit features on the scale envisaged (measures 100 to 102) that would be necessary to verify the accuracy of the result (measures 107 and 108).

Part 8 (Nedap letter of 9 June)

Issue 10: Usability Issues

Nedap Comment: R.9: We would like to know which usability issues the Commission is referring to.

CEV Response: The usability issues referred to here are those set out in the Commission's principal findings concerning the voting machine in section 3.2.1(*d*) of Part 3. These issues relate mainly to behaviour of the user interface that is inconsistent or that may cause voters to cast their ballots in a precipitate or unintentional manner, thus diminishing the accuracy with which voters' true intentions are recorded. The issues concerning secrecy are fewer and are of lesser concern. The

Commission has indicated that many of these issues can be addressed by amendment of the embedded C code software or by minor modifications to the design of the voting machine hardware.

Issue 11: Independent Review of Requirements and Specifications

Nedap Comment: R.19: The Department of the Environment, Heritage and Local Government has the knowledge and skills to specify the requirements and specifications of the system.

CEV Response: The Commission acknowledges the role of the Department to date in developing requirements and specifications of the system. However this recommendation relates to the important additional requirement for independent review of the adequacy and clarity of these requirements and specifications before any further independent analysis and testing of the system is carried out.