Questions to DoEHLG
Responses
Comments

on the

Powervote / Nedap / Groenendaal
Electronic Voting System

proposed for the Local and European Elections in June 2004
by the Department of the Environment, Heritage and Local Government

J P McCarthy **BSc FICS MIEI**
Chartered Engineer
Management Consultant
Election Agent

Original	Thursday 18th December 2003
Responses	Friday 27th February 2004
Comments	Monday 15th March 2004

Preface

This document contains the original text of my questions to the DoEHLG with the Department's response inserted after each topic indented and shown in grey.

The purpose of the original document was to list some questions which arose on my examination of the proposed Electronic Voting system.

Note on Headings

The original document listed 41 topics under which there were 132 detailed questions.

For clarity I have renamed the headings from "Q1." to "Topic 1." etc. and for ease of reference I have added an individual question number to each of the original detailed questions.

Joe McCarthy

Email	joe.mccarthy [at] arkaon.com
Phone	01 607 7116
Mobile	086 245 6788

Table of Contents

Topic 1. Department Response

I received the Department's response by post on Tuesday 2nd March 2004. The document has no date, no author, no page numbers nor does it contain contact details.

The response is entirely inadequate. I did not receive an invitation to engage with or enter dialogue with the Department or the experts contrary to the commitment made by Mr Niall Callan, Secretary General, on December 18th 2003 to the Oireachtas Joint Committee on the Environment.

Unanswered Questions

The Department's response has ignored the following 84 questions:

1	Question 1
2	Question 2
3	Question 3
4	Question 5
5	Question 6
6	Question 7
7	Question 8
8	Question 9
9	Question 12
10	Question 16
11	Question 20
12	Question 21
13	Question 22
14	Question 24
15	Question 28
16	Question 29
17	Question 32
18	Question 33
19	Question 34
20	Question 35
21	Question 36
22	Question 40
23	Question 41
24	Question 42
25	Question 43
26	Question 44
27	Question 45
28	Question 48
29	Question 50
30	Question 51
31	Question 52
32	Question 53
33	Question 56
34	Question 57
35	Question 58
36	Question 59
37	Question 60
38	Question 61
39	Question 62
40	Question 63
41	Question 64
42	Question 65
43	Question 67
44	Question 68
45	Question 69
46	Question 70
47	Question 71
48	Question 72
49	Question 73
50	Question 74
51	Question 75
52	Question 76
53	Question 78
54	Question 79
55	Question 80
56	Question 82
57	Question 86
58	Question 90
59	Question 91
60	Question 93
61	Question 94
62	Question 95
63	Question 96
64	Question 98
65	Question 99
66	Question 100
67	Question 101
68	Question 102
69	Question 103
70	Question 104
71	Question 108
72	Question 113
73	Question 114
74	Question 115
75	Question 116
76	Question 117
77	Question 118
78	Question 125
79	Question 126
80	Question 127
81	Question 128
82	Question 129
83	Question 130
84	Question 132

Misleading responses

The responses for the following 5 topics are quite misleading:

Topic 28. Sabotage outside Irish jurisdiction

This is **the most misleading answer** in the Department's response. It seeks to avoid the clear constitutional issue of who has responsibility for accuracy in casting, collecting and counting the votes of the Irish people.

> 28 What are the risks of sabotage due to the manufacturing and programming of the voting machines outside the jurisdiction of the Irish courts?
>
> The voting machines are extensively and thoroughly tested, both by the manufacturer during production and by the returning officers upon delivery to ensure that all components are functioning correctly. The voting machines are stored in secure locations by returning officers.

> The voting machine will be programmed in the State (at constituency level by the returning officers). Accordingly, control of the programming will fall within the jurisdiction of Irish courts.

The programming referred to is clearly the programming of the software in the Voting Machine by Nedap and the programming of the IES software by Groenendaal.

Both manufacturing and programming are done in Holland clearly outside the State.

Both are clearly outside the jurisdiction of the High Court.

To suggest that the Returning Officers "program" the system is a distortion of the word in the context of this question.

Topic 5. MS Access Database

The Department is mistaken in its view that IES is not an enterprise application. The IES application is critical to the conduct of all elections in Ireland and its accuracy and reliability can only be classified as a safety-critical system. Microsoft recommends against the use of Access for just such systems.

> 5 Use of MS Access
>
> As the Integrated Election Software (IES) application operates on a single, stand-alone computer, with a single user and which is not shared by any other process, the Department does not consider the IES to be an "enterprise" application. It should be noted that the database is not the primary repository of the vote data – the ballot modules are, and these must be preserved for a period of six months following the election(s).

The MS Access database is precisely where the votes are held for the entire process of reading in, reconciling, mixing and counting. During the count it is THE primary repository of the vote data. The question has nothing to do with the Ballot Modules.

Topic 20. Vendor Assurances and Indemnities

The answer given avoids the question of compensation for discrepancies.

> 20 How confident are Powervote and Nedap in the security and reliability of the product? What compensation is proposed in the event of major discrepancies in the elections?
>
> Powervote and Nedap have the utmost confidence in the security and reliability of their system which has been in use in The Netherlands for more than 15 years, and also in parts of Germany. There has never been any incident of lost votes and a full audit trail enables verification of data stored.

There is no audit trail for each vote in this system and to suggest that there is "a full audit trail" is untrue. Without an external audit mechanism how can "utmost confidence" be established?

Topic 16. External Reviews

Essentially, no external reviews of the computing aspects of this system were undertaken.

> 16 External security reviews undertaken
>
> The Department engaged Zerflow Information Security to undertake a security assessment on the security threats to a voting machine in a polling station before the pilot elections. Their report made some recommendations and suggestions to further strengthen the security arrangements.

Zerflow reviewed physical security of the Voting Machine only. No external reviews of cryptographic techniques, computer security or formal code development methods were done.

Topic 33. Haste and Cost

Initial estimates of overall cost based on materials released under FoI show that the capital cost is about half the overall cost.

Major additional costs over the life of this system include:

- Publicity
- Control Operator staff
- Storage
- IT support

> 33 What is the rush with implementing the new system? Can you define the net benefits to the public for this investment?
>
> We are not rushing into the implementation of this new system of voting and counting. In fact, the Department has been working to procure, develop and test this new system in a measured and thoroughgoing manner since 1998. In addition to the independent certification and approval of the new system by internationally recognised institutes and firms, the new voting system was extensively piloted at the 2002 General Election and at the Nice 2 referendum, with over 400,000 voters now having used the system. The reaction of users has been overwhelmingly positive. **Neither has a significant complaint or challenge been made to the Department by any candidate or voter** in the constituencies covered by electronic voting about the fairness or integrity of the process.
>
> The four main benefits to the new system are:
>
> - ease of voting for the electorate,
> - inadvertent spoiled votes are avoided,
> - more accurate and timely results can be produced, and
> - improvements in electoral administration.
>
> . . .
>
> The **vast bulk of the expenditure on this project is a once-off capital expenditure** to purchase the voting machines, which have a life-span of some 20 years. It is expected that substantial savings will be made in electoral administration, particularly surrounding the count procedures.

Increasing levels of challenge have come from myself and others since I made my first FoI request on 18th October 2002 which was *before* the Nice 2 Referendum.

The Department admits that no cost benefit analysis has been done.

New Information

Some new information released was as follows:

1. Four employees of Nathean have seen the IES source code.
2. Groenendaal Bureau BV is responsible for the election management software.
3. The Department has yet to finalise the software contract. [The Minister in a Dáil reply on Thursday 4th March 2004 said: "*The estimated cost of the system software is €467,000. Training is ongoing and cost details are not yet available.*"]
4. No decision has been made whether to acquire or licence the source code. [Clause 10.1.2 of the Powervote / Nedap contract explicitly retains ownership of the Embedded Software in the Voting Machine as the confidential information of the Suppliers.]
5. There is no digital signature on each vote.
6. The vote data is written into the backup Ballot Module after the poll is closed.
7. Neither ERS nor Nathean are internationally accredited. Zerflow was not mentioned in the context of accreditation.
8. The first 100 machines were recalled to Holland for a replacement component.

Topic 1. Experts

How many people have seen the code?

Q. 1. In Groenendaal Bureau
Q. 2. In Powervote
Q. 3. In the Department
Q. 4. In Nathean

These are the ONLY people who can comment on the accuracy of the compliance with Part XIX of the 1992 Electoral Act.

Response

> 1 How many people have seen the code?
>
> Four employees of Nathean Technologies Ltd (an Irish company based in Dublin) have had access to the IES source code. The staff of Groenendaal Bureau have also had access to the code. The Department has entrusted the architectural code review to expert consultants who were engaged to undertake the task of assessing and verifying that the code is correct and consistent with the purposes of the election software program.
>
> Regarding compliance with the count rules as set out in Part XIX of the 1992 Electoral Act, sufficient staff at the relevant levels and ERS have tested the software to ensure compliance.

Questions not answered

Q1
Q2
Q3

Topic 3. Nedap Voter Number

Q. 5. As stated in the Nathean Database review, why is the VM voter number retained in the Access database after the mixing of the votes?
Q. 6. Given that this number is retained would this provide the basis for checking the electronic record against a VVAT paper record even AFTER the mixing?

Response

> 2 Nedap Voter Number – why is the voting machine voter number retained in the Access database after the mixing of votes? Does this provide a basis for checking the electronic record against a VVAT paper record even after the mixing?
>
> The voting machine voter number does not relate to the order in which the votes were cast but rather to the order in which the votes were located in the ballot module and read in from it. As the votes are stored in a random order in the ballot module, it is not possible to associate any vote in the system with a voter, thus preserving the secrecy of the ballot.

Questions not answered

Q5
Q6

Topic 4. Ownership of design and code

The RFT says:

> "8.4 Software
> All software paid for and developed to Department's specification will be the property of the Department."

So the Department owns any code paid for.

Q. 7. What are the details of the draft contract?

Q. 8. Who should own this software?

Q. 9. There can you please supply the source to us for review?

Q. 10. Please explain Mr P Greene's comments to the Joint Committee re the question of licence versus purchase of this code.

Response

3 Ownership and design of the source code

As set out in the request for tenders document, the Department retains the option to either purchase or license the election management and count software. The Department is currently finalising the software contract and will take into account the benefits or otherwise of purchasing the software. In the event that the source code is licensed, a full copy of the code will be held in escrow.

As stated by the Secretary General of the Department at the session of the Joint Committee on Environment and Local Government on 18 December 2003, the Department's primary concern at this stage is to guarantee to the public a system that is reliable and trustworthy. In this perspective, the making available or otherwise of the source code to third parties is a secondary issue, and one that raises issues of commercial sensitivity and security.

The Department will not be in a position to consider acquiring full rights to the code until October 2004 when the system, including a module to cover the presidential election, will have been fully completed. The Minister has stated that, at that stage, he will address all issues regarding the public interest in permitting wider access to the source code, taking into account both security concerns and intellectual property rights of the software designers.

Questions not answered

Q7
Q8
Q9

Topic 5. Returning Officers

Q. 11. What is their responsibility?
Q. 12. Have they the necessary expertise in computer systems?

They purchase the machines from Powervote on the recommendation of the Minister.
Q. 13. Who then owns them?
Q. 14. What team of engineers maintains them?
Q. 15. Where are these engineers based? UK? Holland? Ireland?
Q. 16. What expertise is needed before the election? During the count? Afterwards?

Response

4 What is the role and responsibility of returning officers? Who purchases and maintains the voting machines and software? What expertise is available to them?

The responsibilities of returning officers are set out in the various electoral legislative codes. They are independent in the performance of their duties and are statutorily empowered to run polls in this country. The Department's role is to facilitate and assist them in carrying out these duties, and provide the necessary guidelines and information on all aspects of electoral administration.

The voting machine and software equipment is acquired by returning officers on behalf of the State. There is no annual maintenance on the voting machines, except for normal wear and tear arising from their use. Unlike some US voting machines, periodic re-charging is not required. Where necessary, support and maintenance services for the hardware and software will be set out in the contracts. Nedap are contractually obliged without further payment to provide a maintenance service and employ their technical and engineering staff to repair these machines until the end of 2007. These engineers are based in the main offices of the machine manufacturers in Groenlo in the Netherlands, but are available to travel to Ireland to provide on-site support services.

In their role as organisers and holders of polls, returning officers may avail of IT support to assist them in preparing and running polls. The Department has also facilitated their familiarization with the new electronic voting software and hardware by arranging comprehensive training courses and also by providing a "help desk" and regular visits to every area.

Questions not answered

Q12
Q16

Topic 6. MS Access Database

In http://msdn.microsoft.com/library/en-us/dnacc2k/html/acmsdeop.asp
Bill Demas, Microsoft, in a paper dated June 1999 said the following:

> Enterprise applications require scalability, security, and robustness, which can all be implemented with MSDE or SQL Server **but not with Jet**.
>
> For example, if your application needs transaction support, even in the event of a network, server, client computer, or client application crash, you will want to use MSDE or SQL Server.
>
> Conversely, the Jet engine **does not support** atomic transactions: **It does not guarantee** that all changes performed within a transaction boundary are committed or rolled back.
>
> If the system were to go down with Jet, **the database could be corrupt** and you might need to revert back to your last backup copy.

Nobody uses Access for critical databases.
Microsoft themselves recommend the SQL Server code base.

Q. 17. What is the Departments view on the robustness of MS Access?

Response

> 5 Use of MS Access
>
> As the Integrated Election Software (IES) application operates on a single, stand-alone computer, with a single user and which is not shared by any other process, the Department does not consider the IES to be an "enterprise" application. It should be noted that the database is not the primary repository of the vote data – the ballot modules are, and these must be preserved for a period of six months following the election(s).
>
> Decisions regarding the system design and implementation are based on Powervote's accumulated knowledge and experience in running elections since the 1980s. Powervote's view that MS Access is suitable for use as an element of the election management application has been supported by Nathean Technologies. They have evaluated the database with the quantity of data which will be loaded and processed during an election and have concluded that the MS Access database is capable and adequate for the IES system. This view is backed up by experiences in the city of Cologne where more than 4 million votes have been processed across 600 polling stations covering 9 polls without incident.

Questions not answered

--

Topic 7. Protection of messages –Etopup, Lotto, Votes

Universal practice in systems used in Ireland is to use cryptographic techniques to protect the integrity of messages.

Systems in everyday use such as the Lotto and the mobile-phone voucher topups in shops use encryption and MACs.

Q. 18. Have you considered these techniques?

Q. 19. Is there a Digital signature on every vote?

Q. 20. What is the dictionary used in your implementation of Hamming codes in the Ballot Module?

Q. 21. What do you do when an error occurs?

Response

6 Protection of messages

Encryption is not considered necessary because the data is transferred in a closed system, and not over the internet. The votes which are stored in the ballot module of the voting machine are transferred to the stand-alone election specific PC via the programming reading unit (PRU).

Instead of encryption, the system uses redundancy which provides the ability both to detect failures in data and to detect failures in the hardware. The ballot module consists of two completely independent circuits, including a memory chip. Therefore, if one of the circuits breaks down, the vote can still be counted. In each memory chip, a vote is stored twice to enable any detection of any data-line errors. Before writing a vote, an address-line check is performed to ensure that the data is stored in the right address.

There is no digital signature on each vote.

The system uses a nibble-wise Hamming code with distance 3 on every (copy of a) vote. The Hamming distance can be interpreted as the number of bits which need to be changed (i.e. corrupted) in order to turn one nibble into another valid nibble.

If an error occurs, it will be detected and the voting machine will be blocked for further voting. However, the votes stored in the ballot module are still valid and they can still be read in after the close of the polls into a PRU. Any voter confronted with an error message from the voting machine in this way will be given the opportunity to vote on another machine.

Questions not answered

Q20
Q21

Topic 8. Hamming code

Q. 22. With 4 copies of each vote recorded in the Ballot Module, what are the rules when one copy mismatches on being read in to the Count PC?

Q. 23. And when two copies mismatch?

Q. 24. Are these rules implemented in the "Dutch" code module?

Response

7 Hamming Code

The rule for validation of the votes in the ballot module is that, if two out of the four copies of the vote are valid, then the vote is deemed to be valid. These rules are implemented identically in the Dutch version of the system.

Questions not answered

Q22
The response is quite incomplete.

Q24
This question clearly referred to the Memory_Prog and Memory_Read modules which are still written in Dutch.

Topic 9. No ERS European tests

Q. 25. Why has ERS not been asked to test the European Election profile?
These are very large counts of up to 450,000 votes.

Response

8 ERS didn't perform any tests on European election profile – why?

European election count rules are exactly the same rules as for Dáil Elections. The main difference between the European and Dáil elections is the number of votes. ERS has run successful test cases with up to almost 1 million votes.

Questions not answered

--

Topic 10.Testing with Multiple Ballots

Pseudo code is in-complete
Q. 26. Has this been completed?

The flowchart is incomplete.
Written by Nathean not by the software developers themselves
Q. 27. Has this been completed?

Q. 28. Have the developers supplied their versions of the pseudo code and flowchart?

Response

9 Testing with multiple ballots

The pseudo-code referred to in the supporting queries was prepared by Nathean Technologies in 2001 as a preliminary tool to assist the initial code review. It was intended to help the reviewers to gain a better understanding of the business logic which is implemented in the code. The pseudo code was not a deliverable of the code review and so was not required to be completed.

Similarly, the flowchart referred to was produced by Powervote as an preliminary draft document. It has been superceded by the production of the technical specification, and then by the functional specification, in conjunction with the Department. The final document produced is the system manual.

Regarding multiple ballot counts, a separate count is carried out for each individual poll. PTB has undertaken extensive testing and confirmed that the votes are properly stored in the ballot module in a multiple poll situation.

Questions not answered

Q28

Topic 11.End-to-end Testing

On Wednesday 17th December 2003, I reviewed 5 large files of correspondence concerning the EMS testing, the ERS testing and the IES testing.

Q. 29. There was NO record of an end-to-end test plan.

One record showed that a small number of votes (less than 20) were entered for a few candidates and moved through the system to a final count.

Response

10 End-to-end testing

PTB, the National Institute for Science and Technology in Germany, has specifically tested the voting machine to ensure that the votes cast on a ballot paper (i.e. by pressing the preference buttons and the "Cast Vote" button) are stored correctly in the ballot module. In addition, the count software has been tested by ERS (Electoral Reform Services) to ensure that it

> implements the PR/STV count rules. End-to-end testing is also carried out by Powervote prior to the release of software to the Department.
>
> The software has also been tested for functionality by the Department and returning officers. This has included full test runs of mock elections. For example, votes from actual local election ballot papers were entered on a voting machine and counted electronically. The results of these tests were compared to the actual count results for those elections and were satisfactory, subject to variations because of the mix. There is scope for further exercises of this kind to provide confident demonstration of the system's performance.

Questions not answered

Q29
PTB are irrelevant to end-to-end testing since they only tested the VM.
ERS are irrelevant to end-to-end testing since they only tested the IES count software

What testing did Powervote undertake. Please provide details.

The Department stated that the "Buncrana UDC" test of 2483 votes had tested satisfactorily. Please give further details.

Topic 12.Risk Analysis

Q. 30. Has a formal risk assessment been carried out?
Q. 31. On the VM?
Q. 32. On the EMS?
Q. 33. On the IES?
Q. 34. Can we have a copy of each?

Q. 35. What risks were identified?
Q. 36. What steps have been taken to reduce or eliminate them?

Response

> 11 Has a formal risk analysis been carried out?
>
> Extensive risk analysis as been carried out on the voting machine, and various analyses are set out in the following reports:
>
> - Reliability of the voting machine (report version 1.1);
> - Failure Mode and Effect Analysis (FMEA): Test document no. 9556583.19.11; and
> - Hardware worst-case analysis: (Hardware design document: version 1.01).
>
> As these reports contain extensive testing and sensitive analysis on the voting equipment, which would be of great commercial interest to competitors and other suppliers, copies of these reports are not generally available, as stated in a letter from Nedap to the Department in February 2003.

Questions not answered

Q32
Q33
Q34
Q35
Q36
This answer does not address the question of risk analysis on IES and EMS.
Has any such risk analysis been carried out?

The answer does not indicate that any actions were taken to mitigate identified risks.

Topic 13.Certification

Q. 37. List the certificates issued.

Q. 38. List the accreditation of the certifying agency.

Response

12 List the certifications that have been issued and the accreditation of the certifying agencies.

The following reports and certificates have been issued by the test institutes:

- ERS: Software Validation Report 2003
- KEMA Certificate: 2028725.01
- KEMA-IEV Certificate: 4999018.03
- PTB Declaration of Conformity: PTB-8.33-PA-072/03
- TNO report: 03031001.EMC
- TNO report: R031362/018-40321
- Nathean Technologies: CS-03-0011

Electoral Reform Services – ERS have a world-wide reputation and are the UK's leading elections management company, with an unrivalled track record and expertise both in conducting STV elections generally and specifically in validating STV software. ERS is unaware of any formal qualifications to provide such certification

Physikalisch Technische Bundesanstalt (PTB) – the accreditation of this internationally acknowledged institute is under ISO/IEC 17025. Their accreditation reference is DAT-P-109/01-00

TNO – as with PTB, TNO are accredited under ISO/IEC 17025, and their accreditation reference is L 396.

KEMA – similarly, KEMA are accredited under ISO/IEC 17025, and their accreditation reference is L 022.

Nathean Technologies – Nathean Technologies is an independent Irish software company.

Note: Copies of all the latest reports on the various tests and assessments carried out on the electronic voting system are available for reference and downloading on the Department's dedicated election website – www.electronicvoting.ie

Questions not answered

--

Topic 14.Power failures

Q. 39. What precautions have been taken in the VM?

Q. 40. Please provide more details on the debate concerning the interim storage of the vote in the Xicor chip.

Q. 41. What precautions have been taken in the IES PC?

Response

13 What precautions in the voting machine have been taken in the event of power failures? Also please provide more details regarding the interim storage of votes in the Xicor chip.

Should the mains power fail, all data is kept safe and intact without the use of batteries. However, stand-by batteries will be provided for each voting machine which will enable the voting machine to operate on battery power.

There are a number of scenarios that can occur when the power fails:
If power fails before the "Cast Vote" button has been activated, the preferences are not stored as a vote in the ballot module, and the voter is given another opportunity to vote.
If power fails during vote storage, the vote (which is protected by Hamming codes) is temporarily stored in the Xicor chip. Once the power has been restored, the vote is then stored in the ballot module.

> The polling staff member who operates the control unit of the voting machine can verify that the vote has been stored, as the total number of votes stored in the ballot module is shown on the display.

Questions not answered

Q40
Q41
This response does not answer the question re the IES PC at all.

Topic 15.Powervote Documentation

There is a no technical documentation for the Powervote Counting system

No manual was sent to ERS for their testing this summer. They had to request one. It is not clear if one was supplied.

Q. 42. Who wrote the system specification?

Q. 43. Where is it?

Reference in PMI report to a Technical Documentation CD – page 8 of the Database Evaluation report dated 14 December 2001.

Q. 44. What is this CD?

Q. 45. Why did the Department not reference it in any of their replies to my FoI requests?

Response

> 14 Powervote documentation
>
> ERS did not receive a manual. However, answers were promptly provided to all their questions (which were only a handful), and no other questions arose during preparations for the comparison testing.
>
> Nathean Technologies received a CD containing confidential technical documentation and subsequent software revisions which required a Non-Disclosure Agreement to be in place. This data is not for general release.

Questions not answered

Q42
Q43
Q44
Q45
Note this question related to my FoI requests.

Topic 16.Nedap Documentation

There is a body of documentation for the Nedap Voting Machine

See list on pages 8 and 9 of ESI1_Software document.

Released records x

Refused records y

Q. 46. Why not release the documents withheld?

Q. 47. Particularly the document entitled:

Reliability of the Voting System ESI1, RBW Teunissen, Ver 1.1 dated October 2001.

Response

15 Why were some Nedap documents refused to be released?

As stated in their letter to the Department, Nedap are concerned that, while the documents sought do not give immediate access to the hardware schematics and software code, it would be possible to derive the internal design structure from these documents. This information would enable a competitor to design and develop a comparable voting system to market against the Nedap model. Furthermore, the contents of these documents is comprehensible only to technicians, and it was considered that it was more practical for people to consider the test reports produced which gives a broader and simpler explanation of the system structure and functionality.

Questions not answered

--

Topic 17.External Reviews

Q. 48. Has your system been reviewed by a large number of outside security experts?

Q. 49. If so, who?

Q. 50. What are their credentials?

Q. 51. Do their areas of expertise cover a wide area of specialities?

- within the discipline of cryptography
- computer security
- formal code development methods

Q. 52. Can we see an executive summary of their reports?

Q. 53. Can we have the full reports?

Response

16 External security reviews undertaken

The Department engaged Zerflow Information Security to undertake a security assessment on the security threats to a voting machine in a polling station before the pilot elections. Their report made some recommendations and suggestions to further strengthen the security arrangements. On foot of this report, the Department introduced some refinements of the security features. Following these actions, Zerflow have stated that they are satisfied that the measures taken have dealt with their issues raised in the report and they have no further concerns.

In addition, copies of PTB, TNO, ERS, and Nathean Technologies reports were supplied to Mr. McCarthy and to the Oireachtas Committee on Environment, Heritage and Local Government.

Questions not answered

Q48 – partial – Zerflow only
Q50
Q51
Q52
Q53

Topic 18.Source Code

Q. 54. Do you allow the public to review the security and reliability of your voting system's source code?

Q. 55. If not, why not?

Q. 56. Is the security of your system dependent on your source code being secret?

Q. 57. If so, how do you address the fact that the source code could leak to the public (or to well-funded adversaries)?

Q. 58. And how do you address the fact that an attacker might be an insider who knows the source code?

Response

> 17 Release and availability of the source code
>
> See reply to question 4. [sic – should be Q3]

Questions not answered

Q56
Q57
Q58 – especially for an attack by an insider.

Topic 19.Outside Security Expert Review

Q. 59. Would you be willing to have a panel of outside security experts review the source code for your system?

Q. 60. Would you allow them to publish an executive summary of their findings?

Q. 61. If not, why not?

Response

> 18 Is the Department willing to allow a panel of outside security experts to review the source code?
>
> The Department is satisfied that the independent architectural and code review of the election management and count software undertaken by Nathean Technologies is an accurate and thorough assessment of the source code, and a validation of the integrity and operability of the system.
>
> For those who wish to assess the approach and results of Nathean Technologies's testing, a copy of both reports are available on the Department's dedicated website – www.electronicvoting.ie

Questions not answered

Q59
Q60
Q61

Topic 20.Designer

Q. 62. Who designed and developed the source code used in your systems?

Q. 63. What are their credentials with respect to cryptography and computer security?

Q. 64. Where were they trained?

Q. 65. Have these developers worked on cryptography and computer security in other systems outside of voting software?

Response

> 19 Who designed and developed the source code?
>
> This is regarded by Powervote as company confidential information. The credentials of the election management system and Powervote staff are borne out by the results of continuous independent reviews which span more than 15 years.

Questions not answered

Q62
Q63
Q64
Q65

Topic 21.Vendor

Q. 66. How confident are you in the security and reliability of your product?

Q. 67. Will you "certify" the security and reliability of your product?

Q. 68. Will you offer a full refund, plus "damages," if we purchase your equipment and later find that it is vulnerable to certain types of attacks? (Which types of attacks?)

Q. 69. Will you offer a full refund, plus "damages," if after an election it is determined that more votes were collected than people who voted (on a given machine), but that it cannot be determined which were the legitimate votes?

Q. 70. Will you offer a full refund, plus "damages," if after an election it is determined that your machines reported an inaccurate total (either because of an attack or a system glitch)?

Q. 71. Will you offer a full refund, plus "damages," if after an election it is determined that voters' anonymity was compromised, allowing votes to be bought and / or sold?

Q. 72. Under what other situations would you offer a full refund, plus "damages?"

Response

> 20 How confident are Powervote and Nedap in the security and reliability of the product? What compensation is proposed in the event of major discrepancies in the elections?
>
> Powervote and Nedap have the utmost confidence in the security and reliability of their system which has been in use in The Netherlands for more than 15 years, and also in parts of Germany. There has never been any incident of lost votes and a full audit trail enables verification of data stored.
>
> The Department's preparations for all elections (whether paper based or electronic) have always been premised on the absolute avoidance of major discrepancies, and these are not contemplated either in the present instance. The contractual responsibilities of the manufacturers/developers for the provision of a reliable and robust electronic voting and counting system have been clearly set out. Full observance of the these obligations is required by the Department and all necessary steps will be taken in the event of any default.

Questions not answered

Q67
Q68
Q69
Q70
Q71
Q72

Topic 22.Assurance to the Public

Q. 73. In your system, what can voters do if they feel that their votes were not recorded properly?

Q. 74. Are there any mechanisms for voters to verify their votes are correct?

Q. 75. What happens in the case of a dispute?

Q. 76. Is a manual recount (i.e., not requiring any computer software) possible?

Response

> 21 What procedures and mechanisms are in place to give assurances to voters that their votes are recorded properly?
>
> When preparing the voting machines, the returning officer carries out tests to verify that the location of the candidate's name on the ballot paper is the same as that programmed in the ballot module. In addition, statements produced by the voting machine both before polling commences and at the close of poll confirm that the order of the candidates on the ballot paper is the same as in the ballot module. These documents are part of the election record and can be inspected.
>
> When voters are making their candidate selections on the voting machine, their preferences will appear beside the line of the candidate. In addition, summary candidate details of the last recorded preference is also displayed on the last line of the voting machine display and can be verified by the voter. Voters can check their preferences on all the ballot papers and make changes before pressing the "Cast Vote" button. When this is pressed, the voting machine display will confirm that the vote has been stored. The vote is stored in a random order in the ballot module, which is locked and sealed in the voting machine, to remove any threat of a link between the marked register of electors and the votes recorded in the voting machine, thus preserving the secrecy of the ballot.
>
> Regarding the correct storage of the vote in the ballot module, PTB, the German institute carried out extensive testing on this function and confirmed that it performs all the tasks required and that it has sufficient internal checks to identify any attempted interference.

Questions not answered

Q73
Q74
Q75
Q76

Topic 23.Cosmic Rays

Any system with a large number of machines will experience soft errors due to Cosmic Rays. These high-energy particles occur naturally all the time and will strike the electronics of computer systems in an unpredictable manner.

These particles cause soft errors in memory. The results are unpredictable but their frequency is well understood.

These incidents are called Single Event Upsets (SEU) in the literature.

We have direct evidence of one incident in Belgium and two in Ireland.

Cisco research paper

"Increasing Network Availability" a white paper by P Martson dated 26 May 2000 is available at http://www.cisco.com/warp/public/779/largeent/learn/technologies/ina/IncreasingNetworkAvailability-FAQ.pdf

The following is an extract from this paper:

The use of ECC will decrease the soft FIT rate to a value at least as small as the hard FIT rates (this is influenced by system design and how data bytes are mapped to memory components) which, as described earlier, is one or two orders of magnitude smaller. The FIT values for hard failures are often in the range of 5 to 20, as detailed in Table 2 below.

Table 2: Projected SRAM hard and soft error rates, equating ECC with FIT rates at least as small as hard error rates

	5 FIT	20 FIT	100 FIT	200 FIT
Number of VIP2-50s	**Average Time Between Hard Errors**		**Average Time Between Soft Errors**	
	With ECC		***Without ECC***	
10	71.35 years	17.84 years	3.57 years	1.78 years
20	35.67 years	8.92 years	1.78 years	10.7 months
50	14.27 years	3.57 years	8.56 months	4.28 months
100	7.13 years	1.78 years	4.28 months	2.14 months
200	3.57 years	10.70 months	2.14 months	1.07 months
500	1.43 years	4.28 months	3.72 weeks	1.86 weeks
1,000	8.56 months	2.14 months	1.86 weeks	6.51 days
2,000	4.28 months	1.07 months	6.51 days	3.26 days
3,000	2.85 months	21.70 days	4.34 days	2.17 days
5,000	1.71 months	13.02 days	2.60 days	1.30 days

Note the value highlighted at the bottom right. This predicts an SEU every 1.3 days in a population of 5,000 machines.

> The VIP2-50 supports 4 to 8 MB of SRAM and 32 to 64 MB of DRAM not unlike the amount of memory used in the IES systems.

Q. 77. Since we have some 6000 to 7000 machines in the IES system in use can we expect an error every day?

What precautions have been taken by the designers?

Q. 78. In the VMs?

Q. 79. In the Count PCs?

The Schaerbeek Incident.

Le collège a été prévenu d'un incident à Schaerbeek le 18 mai à 23h30.
4096 more votes counted than cast.

At a polling station in Schaerbeek in Belgium on 18th May 2003, a candidate received more votes than his party list.

See http://wiki.ael.be/index.php/ElectronicVotingRandomSpontaneousBitInversion
for details.

The Belgian e-voting expert David Glaude reports an incident with e-voting in Belgium. Not widely published it took place on 18 May 2003, in the municipality of Schaerbeek. The total number of preferential votes cast for a specific candidate was higher than the total number of votes for his list.

A series of tests was conducted on the computer of the president of the voting committee, but the error could not be reproduced. The difference in votes was exactly 4.096, leading the research-team to the conclusion that the error was probably due to a spontaneous inversion of a binary position in the read-write memory of the PC.

The Belgian e-voting system is fairly complex, with a blank magnetic card that every voter has to insert into a voting machine. After voting, the card must be entered into a ballot-box. Attached to the ballot-box is a computer with a floppy-drive. The voting-results are written on a floppy-disk.

See the official report (in French) from the Collège d'Experts at
http://www.poureva.be/article.php3?id_article=32

An investigation began on May 19 in the presence of the president from canton, representatives of the SPF Intérieur, companies Steria and Bureau Van Dijk and college of experts.

5.3.7.3 Conclusions of the college on the incident of Schaerbeek:

Since no error was found in the software, and considering the internal structure of the program, the college concludes that the error was most probably caused by a spontaneous and random inversion of a binary position (this phenomenon is abundantly described in the specialized literature).

BM 367 Limekiln

A failure occurred with Ballot Module, number 367 of Dublin South West – used at St Paul's Senior and Junior Primary Schools, Limekiln.

It had a "*blocked - checksum not in order*" failure and was sent "*to Nedap for a report*".

This failure shows that computer systems do fail sometimes. This is one part of the Irish Electronic Voting system that has failed.

It may have failed due to a "Single Event Upset".

Error 7002 Xicor chip write and failed readback.

On 14 Dec 2002 Powervote reported an eplanation for an error 7002 in Voting Machine P3D000578 used in Dubln West for the Dail 2002 election. Staff at the polling station reported that the machine had this error.

The explanation was *"...the Xicor chip wrote a code and it detected that the read back was not correct".*

This almost certainly was caused by an SEU. Powervote offered no further explanation.

See also http://www.pcguide.com/ref/ram/err.htm for details of memory protection schemes including parity, false parity and ECC.

Note that the recommended PC for the Returning Officers does NOT support ECC.

Conclusion: The Irish voting system will suffer one of these events in every election.

Q. 80. What does the Department propose to do about this?

Response

22 What precautions are being taken to deal with the incidence of cosmic rays?

The probability of an error due to cosmic rays has been calculated as being once in every 12 elections, where 6,500 voting machines are in operation during 16 hours of polling. Nevertheless, the votes in that machine will still be securely recorded and retained, due to the redundancy inbuilt into the system. Four copies of each vote is recorded separately and randomly in the ballot module to prevent any damage or interference with the vote data.

On a more technical level, the frequency of SEUs is mentioned in the Cisco document. In response to the question of how often do SEUs occur, the answer is that SEUs are relatively infrequent but are proportional to system memory size. For example, a single VIP2-50 with 8MB of SRAM is predicted to detect data with bad parity in SRAM once in 18 to 36 years. As the number of devices in a network increases, the predicted SEU occurrence increases proportionally.
Note:
The memory size of the voting machine is less that 1 MB (RAM + EEPROM + EPROM + FLASH). Therefore, it is predicted to be affected by an SEU once in 144 to 288 years, since that is proportional to memory size.

Calculation of the failure rate of one voting machine due to SEU:
1/(144 years x 365 days x 24 hrs) = 793 FIT

With 6,500 machines operating during 16 hours in a polling day, the probability that an error can occur is:
793 FIT x 6500 x 16 = 0.08 failures

With regard to Mr. McCarthy's claim that he has "direct evidence of SEU incidents, 1 in Belgium and 2 in Ireland:
Ballot Module 367 Limekiln
Message: "blocked – checksum not in order"
Cause: This error occurred after the ballot module was transferred from the returning officer to the Referendum Returning Officer for deletion after the 6-month retention period. The ballot module was transported out of its proper storage case and was damaged in transfer. Investigation showed a problem with one of the solder joints, and not as a result of an SEU. However, it should be noted that the votes stored on the ballot module were properly read for the Nice 2 Referendum in October.

Voting Machine No. P3D000578
Message: "7002: event_xicor_verify_fout_hist" (i.e. a write failure occurred, during the logging of an event in the XICOR memory).
Cause: At Nedap, the machine functioned properly, with several read-write tests being performed satisfactorily. This can have had several causes. The normal failure rate of the XICOR device is 155 FIT. Once again, the storage of the votes in the ballot module was not affected and all the votes were properly read in.

The conclusion that computer systems do fail sometimes is correct. The main goal for the design of the voting machine was not only to avoid possible failures but to detect any possible failure during the election process and protect stored votes in a very secure way by redundancy.

Questions not answered

Q78
Q79
Q80

Topic 24.Multi-user or not

Statements to committee that PCs will be standalone.

There detailed provisions in the system and in the instructions and in the testing for multi-user implementation.

Q. 81. Which is it?

Q. 82. What is the performance of a single machine counting up to 450,000 votes in a European Parliament constituency?

Response

23 Will the PCs used in the election be stand-alone or connected to a network?

The PCs used for the election set-up and vote counting are stand-alone machines, complete with anti-virus software. Each one will be "security hardened" for the election, i.e. all unnecessary services and programmes on the PC will be disabled or reconfigured, and will also be equipped with a two-level security log-in procedure to prevent any unauthorised access to the PC. Returning officers will ensure that the election PCs are securely stored and that only authorised access to, and use of, the computers will be permitted.

Nathean Technologies has conducted all source code reviews with the understanding that the system in June 2004 operates as a single-user application and database.

Questions not answered

Q82

Topic 25.Performance

How fast are these machines at reading in the ballot modules?

Q. 83. For General elections?
Q. 84. For European Elections?

Q. 85. How fast are these machines at counting?

Q. 86. Please detail the logistics for the European elections?

Response

> 24 How fast are the PCs at reading the ballot modules, and how fast are they for counting votes?
>
> Each of the election-specific PCs will be security hardened and will have the following specification:
>
> - Intel Pentium 4 Processor
> - Intel 845G Chipset
> - 512 KB Processor Cache
> - 512 MB DDR RAM
> - 40GB Smart Ultra III/100 Hard Drive
>
> In terms of the time it will take to read in a ballot module with, for example, 500 votes stored on it, the processing time is approximately 20 seconds. The time for mixing the votes and then for the counting will depend on the volume of votes. For the smaller electoral areas (e.g. LEAs, Town and Borough Council elections), the time required to mix and then count will only be 1 or 2 minutes. In the European elections, where there may be over 500,000 votes being counted, this process may take 10 to 15 minutes

Questions not answered

Q86

Topic 26.Maintenance free statement

Machines have already been sent back to manufacturers to have a chip replaced.
Q. 87. Which machines?
Q. 88. How many?
Q. 89. Why?

PCs do not last 20 years.

Q. 90. Has an assessment of the engineering maintenance been done
Q. 91. What are the results?

Response

> 25 Has an assessment of engineering maintenance been done? Why have some machines been sent back to Nedap for upgrading?
>
> Following the pilot elections in 2002, on foot of feedback from voters, returning officers and our security advisers, the Department decided to improve some aspects of the voting machine, such as making the display bigger and brighter (use of LEDs vs. LCDs) to make it even more user–friendly for voters, and also to slightly modify the design to aid transport (e.g. provision of extra handles to enable two people to carry it). The 1000 machines that were used in the pilots were shipped back to the factory for up-grading and refitting, and these machines have since been returned to the relevant returning officers for use at the June elections.
>
> The manufacturers also undertake on-going reliability tests (ORTs) on all the components that comprise the voting machine. This ongoing testing enables the company to maintain the highest levels of quality control and minimise the risk of malfunctions. Early in the production of the voting machines, ORTs during production showed a possible component failure. The potential failure may not have ever occurred but, given the 20-year life of the voting equipment, it was decided, as a precautionary measure, to recall the first 100 voting machines delivered to Ireland for replacement of the part in question. The voting machine itself is maintenance-free.

Questions not answered

Q90
Q91
The VMs may be maintenance free but PCs certainly are not.

Topic 27.Petition Logic

This complex aspect of the software had not been developed or tested in the records I had sight of.

Q. 92. What is the current state of development and testing?

Q. 93. Is it still proposed to re-adjust each ballot to remove preferences for dis-qualified candidates?

Q. 94. If so, does this procedure interfere with the ballot as cast by the voter?

Q. 95. Is this constitutional?

Response

26 Has the Department undertaken testing of the petitions functions in the software?

The development and testing of the petitions software by the Department is complete.

As regards disregarding all preferences recorded for an ineligible candidate, Rule 7 (5) of the Third Schedule to the Electoral Act 1992, as substituted by section 47 (c) of the Electoral Act 2001, provides that, at the hearing of a Dáil election petition:

> “Where votes are counted afresh …, the court shall cause the preferences recorded for any person who, with respect to the relevant Dáil election , is found by the court not to have been eligible for election to the Dáil to be disregarded…”

The petitions software has been programmed to implement this measure, if the court so directs.

Questions not answered

Q93
Q94
Q95

Topic 28.Vandalism

Superglue, magnetic fields, chewing gum, brute force, a penknife?

Q. 96. What risks have been assessed?
Q. 97. What precautions have been taken?

Response

27 Has there been a risk assessment for acts of vandalism? What tests have been undertaken?

There have been no acts of vandalism recorded in the history of the voting machines’ use. The risks that have been assessed are damage to the membrane switches and to the display.

Special membrane switches overlay has been developed to withstand vandalism (e.g. sharp things) to a certain extent. On the voter panel, there are no moving parts, so this avoids any problems with glue or chewing gum arising. The display is also covered with a thick plastic window to avoid direct damage to the display itself.

The ballot module is locked and not directly accessible to the voter. Furthermore, electromagnetic immunity has been tested according to European Standard EN 61000-4-2: 1995. Moreover, every machine is production tested with electrostatic discharges of 16kV.

Questions not answered

Q96

Topic 29.Sabotage

Manufacture and programming is done outside the jurisdiction of the Irish Courts.

Q. 98. What risk does this pose to the Irish voting system?

Response

> 28 What are the risks of sabotage due to the manufacturing and programming of the voting machines outside the jurisdiction of the Irish courts?
>
> The voting machines are extensively and thoroughly tested, both by the manufacturer during production and by the returning officers upon delivery to ensure that all components are functioning correctly. The voting machines are stored in secure locations by returning officers.
>
> The voting machine will be programmed in the State (at constituency level by the returning officers). Accordingly, control of the programming will fall within the jurisdiction of Irish courts.

Questions not answered

Q98
The programming referred to is clearly the programming of the software in the Voting Machine by Nedap and the programming of the IES software by Groenendaal.

Both clearly outside the State.

Both clearly outside the jurisdiction of the High Court.

To suggest that the Returning Officers "program" the system is a distortion of the word in the context of this question.

This is **the most misleading answer** in the Department's response. It seeks to avoid the clear constitutional issue of who has responsibility for accuracy in counting the votes of the Irish people.

Topic 30.Capacities – 5 elections - 56 candidates – 18 LEDs

Q. 99. What are the limits on the VM,
Q. 100. and in the IES?

For local elections candidates need 15 registered voters for nomination.

Q. 101. If, say, 1500 people nominate 100 candidates, what happens to this system?

The constitution permits this.

Originally 28 Buttons / LEDs per column – now it is 18.

Q. 102. So does the max of 56 candidates per election now become 36?

Response

> 29 What are the limits on the voting machines and IES software? What happens if there are more than 36 candidates in a election?
>
> The voting machine has five columns which enables up to five different ballot papers to be used simultaneously. There are 18 rows in each column, but where the number of candidates exceeds 18, a second column can be used for that election, and the candidates will be split evenly between the two. If the number of candidates were to exceed 36, a third column would be used, and so forth. The highest number of candidates at the 1999 local elections was 26.

Questions not answered

Q99
Q100
Q101
Q102

Topic 31.Secure Coding Methods

Q. 103. Were any used in developing these systems?

Q. 104. Which ones?

Q. 105. Was Bruce Schneier consulted?
Q. 106. Was Ross Anderson consulted?

Q. 107. If not, why not?

Response

30 Were there any secure coding methods used in developing the systems?

The credentials of Nedap and Powervote's system and staff are borne out by the results of continuous independent reviews which span more than 15 years. Neither Bruce Schneier nor Ross Anderson were consulted as it was not considered necessary, given the extensive independent testing that has been carried out on all aspects of the Nedap-Powervote system.

Questions not answered

Q103
Q104

Topic 32.Security

Q. 108. What security is used to protect each vote in the Access database?

Security by obfuscation is no security.

Example is the A5 algorithm used in the GSM standard. The manufacturers did not allow open review – it has now been cracked.

Response

31 What security is used to protect each vote in the access database?

As the software is a critical element of the system, the developers have designed their own security and integrity procedures, which is used in all versions of the election management (IES) programme.
Within the procedures of IES, the votes are checked and verified at more than one point, e.g. the Voting Machine produces a printed statement, there is a check done at the time the ballot modules are read in, and the reconciliation section of the process contains the list of votes per polling station.

Questions not answered

Q108

Topic 33.Development model

The Nathean Code Review Guidelines, dated 14 December 2001, on page 3 says:

> "Typical code reviews should address the following questions:
> 1. Does the code implement the design as specified in the design document?
> 2. Does the code have unspecified side effects?
> 3. Does the code follow your style guide
>
> As PMI Software is not the developer of the system, we cannot establish if Powervote's style guide has been followed so we have concentrated on 1 and 2"

Nathean therefore could not carry out task 3.

Q. 109. Does this mean that nobody has checked the style guide used by Powervote?
Q. 110. Can we have a copy of this style guide?

Response

32 Is it possible to check the style guide of the software used by Powervote in the development of their IES software package?

The statement quoted in Nathean's Code Review Guidelines related to the code review process and not the development model. An essential element of a code review is to establish if the programmers have followed any organisation-specific coding or style specifications, aside from general best practice. In this case, Powervote did not specify any alternative style guide and therefore best practice has been adopted as the style guide.

Topic 34.Haste

Q. 111. Why is there a rush to implement?

Paper voting for over a century has resulted in a stable situation with:

- Detailed Statutes
- Established case law
- Vast experience
- Public ownership of the process

Q. 112. Can you define the net benefits to the public for this investment?
Q. 113. Can you cost them?

Response

33 What is the rush with implementing the new system? Can you define the net benefits to the public for this investment?

We are not rushing into the implementation of this new system of voting and counting. In fact, the Department has been working to procure, develop and test this new system in a measured and thoroughgoing manner since 1998. In addition to the independent certification and approval of the new system by internationally recognised institutes and firms, the new voting system was extensively piloted at the 2002 General Election and at the Nice 2 referendum, with over 400,000 voters now having used the system. The reaction of users has been overwhelmingly positive. Neither has a significant complaint or challenge been made to the Department by any candidate or voter in the constituencies covered by electronic voting about the fairness or integrity of the process.

The four main benefits to the new system are:

- ease of voting for the electorate,
- inadvertent spoiled votes are avoided,
- more accurate and timely results can be produced, and
- improvements in electoral administration.

By extending the facility to vote electronically to all parts of the country for the European and local elections in June 2004, we can enable the electorate to enjoy the many benefits of electronic voting now; the alternative would be to delay these benefits for several more years, given the cycle of the various elections.

In terms of the net benefit of the system, it should be understood that, while cost is an important consideration, it was not the sole determining factor in the Government's approval of the new system. The accuracy, reliability and security of the electoral process has been of paramount importance in selecting and developing an appropriate electoral system. The system chosen incorporates security and audit features (both internal and external) at all stages of the election process from initial set-up of a poll to the production of the count result.

The vast bulk of the expenditure on this project is a once-off capital expenditure to purchase the voting machines, which have a life-span of some 20 years. It is expected that substantial savings will be made in electoral administration, particularly surrounding the count procedures. The extent of the savings is dependent on the number of national polls held and hours and days appointed for such polls during the twenty-year period. In some years, two or three polls may be held (as in 2002), while there may be no polls held in other years (e.g.

> 2003). Therefore, it is not possible to calculate what the precise savings will be made over the life of the machines.

Questions not answered

Q113

Topic 35.Cost

Q. 114. The Department has not done a cost analysis.

Every VM needs a control operator – this is one more person at each polling station.

Q. 115. What are the explicit costs for the IES software part of the contract?

The voting machines cost € 5,008 each plus VAT with a 10% discount for 6000 machines.

Response

> 34 Has the Department done a cost analysis? What are the explicit costs for the IES software part of the contract?
>
> Negotiations on the final costs of the software elements of the election management program are ongoing and are dependent on the decision as to whether the Department decides to license or purchase the code. The costs will be fully set out in the contract when it is completed.

Questions not answered

Q114
Avoids the question of cost of control operators – up to 6,200 additional staff (less some 2,500 counting staff) – a net increase of up to 3,700 staff per poll.
Q115

Topic 36.Indemnity

Q. 116. Will Powervote indemnify the Irish people that this system will faithfully implement Part XIX of the Electoral Act 1992 as amended?

Response

> 35 Will Powervote indemnify the Irish people that this system will faithfully implement Part XIX of the Electoral Act 1992 as amended?
>
> Responsibility for the implementation of Part XIX of the 1992 Electoral Act is a matter for the returning officers as set out in legislation. The Electoral Reform Services have carried out comprehensive testing on whether the election management software faithfully implements the PR STV count rules. Their report confirms that the rules are properly applied.

Questions not answered

Q116

Topic 37.Quality

Q. 117. Who is responsible for the quality of the whole system?

It seems that this task has fallen to the Department. They do not have the necessary expertise and must rely on external companies. They have chosen just two: Nathean and ERS.

Q. 118. What tendering process was used to select these two companies?

Response

> 36 Who is responsibility for the quality of the whole system? Does the Department have the necessary expertise to deal with this issue? How were ERS and Nathean Technologies selected as external consultants?
>
> The Department is operating as project managers for the development and roll-out of the electronic voting system. In this role, the Department has had continually available to it the

expertise and services of its specialist agency, the Local Government Computer Services Board. In terms of the individual elements of the system, Nedap is responsible for delivering the voting machine, ballot module, programming reading unit and all related documentation. Groenendaal Bureau BV is responsible for the election management software.

Both Nathean Technologies and ERS were selected following public tender competitions.

Questions not answered

Q117
Q118

Topic 38.C&AG

Q. 119. Has the C & AG done a value for money audit?
Q. 120. What is the result?
Q. 121. Can we have the report?

Response

37 Has the Comptroller and Auditor General done a value for money audit?

No.

Topic 39.Suppliers

Q. 122. Please explain the relationships between

- Powervote Ireland
- Powervote Services Ireland
- Powervote UK
- Nedap
- Groenendaal Bureau

Q. 123. Who owns shares in these companies?

Q. 124. Who gets the profits?

Response

38 Can you explain the relationships between the various suppliers of the electronic system?

Groenendaal B.V. and Nedap N.V. collaborate in the design and development of Election Management Systems over 15 years. Powervote was formed to develop market opportunities in a number of countries, including the UK and Ireland.

Regarding share ownership in these companies, full information including share ownership in public domain. In summary,
Powervote Ireland is registered in Ireland (Ref No. 368097)
Powervote Services Ireland is also registered in Ireland (Ref No. 376596)
Powervote UK is registered in England (Ref No. 3611469)
Nedap BV is registered in the Netherlands (08013836 Handelsregister)
Groenendaal Bureau is also registered in the Netherlands (28062383 Handelsregister)

As with all companies, the profits generated by the company are ultimately distributed to the shareholders, after giving due consideration to the working capital requirements of the company.

Topic 40.Spot Checks

Q. 125. Can we select random VMs for a paper check?
Q. 126. Can we select a random constituency for an audit?
Q. 127. Who should conduct these audits?
Q. 128. Do we need an electoral commission to do this?

Response

39 Can voting machines be randomly chosen for a paper check, and can a constituency be randomly selected for an audit? Is there a role for an electoral commission?

The Government has decided to establish an independent Electronic Voting Commission to verify the secrecy and accuracy of arrangements proposed for electronic voting.

Questions not answered

Q125
Q126
Q127
Q128

Topic 41.Legato – Hot backup

Financial systems used in Dublin use techniques based on Legato Software to ensure a second copy of each record is safely written before the software continues.

Have such techniques been considered here?

Q. 129. For the Voting Machine?

Q. 130. For the counting machine?

Q. 131. Have write only media such as CD-R been considered?

Response

40 Has the use of Legato/Hot back-up systems been considered? Has write only media such as CD-R been considered?

When in use, the voting machine is designed to constantly test the functioning of its major components to ensure that it is functioning correctly. Because there are four copies of every vote stored in two independent memory chips, the storage of the votes in the ballot module is always secure. In the event of any error or malfunction, the voting machine immediately shuts itself down. In such circumstances, a replacement voting machine is provided and voters can use other machines in the building until the replacement is provided.

In addition, when the poll is closed on the voting machine, a back-up of the vote data is made on another ballot module that is stored within the hardware of the voting machine. In the event that a module is damaged or lost in transit to the read-in centre, the spare ballot module can then be accessed and it will contain the same vote data.

Regarding the transfer of data by CD, only CD-Rs will be used so that there will be no opportunity to replace the vote data stored on the customised CDs during transit. Moreover, as with the transfer of paper ballots, the transfer of the vote data on CD will be strictly controlled and monitored by each returning officer.

Questions not answered

Q129
Q130

Topic 42.Dutch Code

The Nathean report pointed out certain modules with dutch comments and function / variables names.

Q. 132. Has a version written in English been supplied?

Response

41 Has an English version of the code modules with Dutch comments and function or variable names been supplied?

All code relating to the Irish version of the IES system has been supplied in English. Nevertheless, Nathean Technologies Ltd. retain the services of a native Dutch senior Delphi developer as part of the review team to assist in any translations as required.

Questions not answered

Q132