Appendix 3B

Summary of Submissions

THE POLICY INSTITUTE, TRINITY COLLEGE DUBLIN

Professor Michael Laver, *Department of Political Science, TCD*
Professor Michael Marsh, *Department of Political Science, TCD*

No.	*Name of person(s) or body*	*Main Points*
1	Patrick O'Beirne	• IT professionals know that only a voter verified audit trail can check accuracy
2	Charles Flanagan	• Should not publish tallies, which would infringe secrecy
3	Ann Burns	• Supports e-voting but wants a provision to spoil the vote
4	Roy Madden	• All computer system have faults and the only way to check accuracy is with an independent audit trail • No indications of a comprehensive independent risk assessment • Testing only on subsections of the system • Needs to be built according to secure software development guidelines (as in NASA), not in home PC environment • Software certified in tests not necessarily the same as the software used in actual election • Is there an audit trail of changes to the software – which is critical
5	David Bateman	• No software can be 100% tested • Software tested against accidental malfunction not deliberate manipulation • Software malfunctions can show up after several years • Parts of the whole system are continuously upgraded – then everything needs retesting (NASA kept 1960s shuttle computers for this reason) • Every upgrade introduces new risks
6	Dr. Roy H W Johnston	• Easy to manipulate any system, so paper trail is essential • Need to use Gregory method for surplus transfers
7	Francis Butler	• Need voter verified paper trail
8	Alan Jones	• Anti e-voting message supplemented by a large number of attachments. All are on e-voting (mostly in the US)
9	John McGinley	• Objections based on secrecy of the ballot that would apply also to paper voting (if a candidate gets zero first preferences, then s/he knows that no voter voted for him/her, and knows your ballot in this sense) • Objections to releasing tally data
10	Jim Harding	• Blank/spoiled ballots will be obvious to poll clerk
11	John Fintan Fitzgerald	• Was a voter who had a problem registering an e-vote in Dublin South in the 2002 referendum: The vote was initially not registered and nobody noticed this until the voter drew it to their attention • From long experience of IT – need a parallel run with a paper trail to validate system
12	Michael and Ethna Viney	• As daily computer users, feel that paper trail is only way to validate system

No.	***Name of person(s) or body***	***Main Points***
13	P.M. Boyle	• Commission not independent since appointed by Government • Commission should make research results available before a decision is made • Commission has insufficient time to make a decision
14	Ben Cranks	• Software should be open source
15	Frank Mason	• Software should be open source • Potential for manipulating program • Need referendum to change to e-voting • No constitutional right to spoil a vote
16	Brendan Farrell	• Cites US research showing problems with no paper trail • Onus on Government to prove system safe
17	Tommy Weir	• Cites problems in Florida 2004 with e-voting • Paper trail the only defence against manipulation
18	Kiernan Burke	• Cites problems in Napa with one of the e-voting machines, causing a recount • Hence need for paper trail
19	Tom Coughlan	• Cites need for paper trail, given €10,000,000 electricity bills
20	Tom O'Seitheacháin	• Cites need for paper trail, will spoil vote otherwise
21	Kiernan Burke	• Cites US research on problems with e-voting
22	Geraldine Bird	• Argues need for paper trail – citing last US presidential election
23	Micheal Mac Biorthagra	• Fears votes could be reconstructed from voting order
24	Aidan O'Hara	• Generally opposed to the use of machines to count votes
25	John Burke	• No way of voter knowing that actual vote is recorded • Fears for secrecy of the ballot • Mistakes by poll clerks could compromise result • Fear for effect of power failure at a busy time
26	George Mullan	• Argues for paper trail – a machine readable paper vote
27	Bobby Carty	• Argues election could be disrupted if more than 40 candidates
28	Thomas Long	• Fears mistake in transcribing postal vote into electronic system
29	Yvonne Slattery	• Blank/spoilt vote will be visible to poll clerk because of need to reset machine
30	Stephen Geraghty	• Argues for paper trail
31	Fergal Shevlin	• The only way to test the accuracy of the system is to have a parallel paper trail
32	Milo Doyle	• Main issue, need for paper audit trail • Secondary issue, software should be open source for public inspection
33	Donal O'Callaghan	• Asks whether there have been final tests of system actually to be used • Asks about protection of memory modules from corruption

No.	*Name of person(s) or body*	*Main Points*
34	Antoin O Lachtnain	• Argues he cannot make proper submission without unavailable technical documentation, source code, test results, operational manuals, contracts with suppliers which he asks the Commission to provide
35	Kieran O'Sullivan	• Argues for Lotto-style paper trail • Argues for extension to internet voting
36	Paul Donnelly	• Citing Florida, argues for paper trail • Argues that source code can be rigged from the inside
37	John Timmons	• Argues for open source code • Argues for paper audit trail
38	Philip Newton	• Unqualified support for new system – "there will be teething problems that I am sure will be ironed out, we should all give it a chance"
39	David Algeo	• Argument that the present system has not been sufficiently tested: o Once it has been "tailored" to a particular constituency/election; o To ensure that all votes cast are included in the count; and o To show that there is no need for a paper audit trail, when this is usual in such applications • Assumes that the decision to dispense with an audit trail arises from the unreliability of hand counting, so that the Government prefers an uncontested result to an audited one
40	Pat O'Flaherty	• Supports introduction of e-voting, to achieve greater accuracy • BUT argues for parallel elections with audit trail to test accuracy
41	Peter Barrett	• Wants assurances that source code will be available and specific Irish modules rigorously tested • Wants information on security against manipulation • Asks about EU endorsement of the use of chosen system for European Parliament elections
42	Mark Wakefield	• "testing will not reveal whether there is an electronic 'back door' which would allow the system to be subverted in the future" • System can be manipulated • Lack of paper audit trail
43	Paul Casey	• Commission Report should set out the people, processes that will ensure secrecy and accuracy • Plus a statement of how results will be audited • Plus full technical evaluation of what is inside the various "black boxes" of the system
44	Raymond McCarthy	• Cites risks of error, failure and manipulation
45	Dáire Mag Cuill	• No computer system is 100% dependable

No.	***Name of person(s) or body***	***Main Points***
		• Therefore need paper trail • Feels it may be technically possible to "bug" machines and read people's votes
46	John Morrison	• Need for a Total Quality Audit Panel for the system • Some suggestions on security
47	Kiernan Burke	• Information on the UK Institute for Information Policy Research
48	Seán Shelly	• "Sceptical that any machine is 100% reliable 100% of the time" • Thus would like audit trail
49	"user"	• Need a referendum to introduce e-voting, excluding non-nationals
50	Donal Kelly	• "it is not realistically possible to test the software to 100% coverage. This means that with the chosen system there will be thousands of lines of code [about] which nobody can accurately say what these lines of code do"
51	John Reid	• All electronic equipment ultimately fails – thus 100% accuracy impossible to achieve
52	Michael Farrell	• Audible beeps when pressing buttons meant that people outside can hear when voter is making errors – violating secrecy • No sense of security that vote cast was vote recorded
53	Michael Prendergast	• No problem with the current paper system • 2002 tests of e-voting not relevant, given subsequent software upgrades • No parallel running of electronic and hand counted systems • Too little time for public to make submissions to Commission • Commission terms of reference should have included "security" • No external validation of results • Transfer of ballot modules more vulnerable to breaches of vote secrecy than that of ballot boxes
54	Meg Dunne	• How will the system work for blind voters? • Will they be able to try it out in advance?
55	Andrew Ogle	• Proposed system no improvement on present one • Given public concerns about new system – forcing it through will increase public distrust of Government
56	Tommy Broughan, T.D.	• "Grave concerns that the key which gives polling staff access to sensitive features on the machine is easily copied and could be abused" • Without paper audit trail, no security that system has not been accidentally or deliberately corrupted • Possibility of wiping the backup cartridge • "a transparent hard copy of each person's vote is critical"

No.	*Name of person(s) or body*	*Main Points*
57	Gerard Lardner	• Need for voter verified audit trail – with specific suggestions for implementation • Need for visible tamper-proofing of voting machines • Need for "demonstrably adequate" protection against double voting
58	A. Leavy	• Need paper verification of each vote – paper audit trail
59	Cllr. Niamh Bhreathnach	• Should advise the Government to "hasten slowly", given the need for public trust • Constituents (older people and IT professionals) have told her they will not vote if the proposed system is introduced
60	Donal O'Callaghan	• Generally favours electronic voting • Objects to proposed system because – o No verification that vote cast is vote recorded, given lack of paper trail o Security problems with transfer from data cartridge to counting computer o Computer counting process prone to unintended error or deliberate manipulation • Thus there is a need for a paper audit trail – else roll out of the proposed system should be deferred • Cites best practice in banking • Suggests adding "none of the above" to get around non-secrecy of blank ballot • Problems with queues for machines at peak times
61	Rory Donegan	• Need for a full risk assessment of the system since… • Every system can be interfered with • Thus need till roll style audit trail
62	Liam J. McMullin	• Need a paper audit trail • Suggests paper voting with votes manually input at counting centre
63	Dermot Dunnion	• Advocates a voter-verified paper audit trail OR • A detailed series of security criteria which should be applied in any testing of the chosen system, including o Independent check by three independent third parties of the final system deployed – down to binary code level o Verification on the day of the poll that all hardware and software are the versions certified o Detailed security checks, risk assessment on possibility of modifying all programs and data • Without these checks, a verified paper trail should be used
64	David O'Higgins	• Voters need a receipt with a unique transaction number, so that they can check their vote was counted (like ATM receipts) • System needs transparent audit trail • Could not recommend a client to install anything like the proposed system

No.	***Name of person(s) or body***	***Main Points***
65	Dr. Michael Purser	• Technical information needed to make informed comments is not available to citizens • Concerns about secrecy – is vote data encrypted for transfer, since this is when it is vulnerable • No way for voter to check his/her vote has been recorded and counted correctly • Apparent "Glaring defects" in current system include: o The need for a voter-verifiable paper audit trail o The fact that there has been no parallel running between the old and new systems • "This is unheard of in any serious situation"
66	Pat Kearney	• Objects, in the name of democracy, to lack of opportunity to spoil vote under e-voting
67	P.J. Kerr	• Suggests security would be enhanced by satellite tracking of each ballot module en route to the count centre • Suggest taking simultaneous copy of vote data on CD ROM before it leaves polling station – to be transported by different route and reconciled with ballot module at count centre
68	The Labour Party	• Begins with a summary of the history of evoting in Ireland to date (sections 2 and 3), and description of the overall system • Section 4 puts the case strongly for a voter-verifiable audit trail (VVAT), on the grounds both of unintended software or hardware failure, and tampering. Without this, the proposed system should not be used. Takes explicit account of the problem in matching hand and computer counts, given the randomisation of ballot selection on surplus distribution, and suggests a solution • Criticises lack of integrated end-to-end testing of system, as opposed to tests of constituent parts, and notes that "random mix" aspect of software was disabled for ERS testing. Thus "the election management software, as it will operate in a real election count, has not been tested" • Criticises lack of formal methods in developing software – essential for safety-critical applications. As a result, suggests that source code must be published, to allow open public review • Discusses possible tampering opportunities and concludes there is insufficient security associated with: o Access to count centre PCs o Verification that software installation on PCs and voting machines is the tested version and o Purchase of ballot modules • Concludes with the "key recommendation" for a voter verified audit trail • For an independent body to take audit and supervisory role and

No.	*Name of person(s) or body*	*Main Points*
		• For "full statistical analysis" and integrated end-to-end tests before any system is implemented
69	Timothy J. Lane	• Feels that the c.1400 test cases used by ERS in published reports is far too few. Was there automated checking of results? • Need for continuous retesting when ANY aspect of the system/software is changed – given interaction effects that often arise • Has it been checked that the system is easy to understand by all types of people? • Need for voter verifiable audit trail • Once finally tested, a "golden copy" of the program is given to the electoral authority and that this, and only this, tested version is used on the day. "It is important that this copy is not left in the control of the vendor" • For a given election, run time software (RTS) must be customised for the machine. An encrypted unique security code should be embedded in each version of the RTS – to allow software to be unlocked on the morning of the poll by a returning officer opening a PIN code in a sealed envelope • The same security routines should be used for the count software
70	Conor Lennon	• Argues for open source software, if accuracy is to be checked comprehensively
71	John Horan	• Argues need for "none-of-the-above" voting option
72	Ingrid Masterson	• Argues that use of system in other countries is no valid test because they use different voting systems and that e-voting is a waste of money
73	James Dillon-Kelly	• "None of the voters I dealt with expressed any anxiety about the security of the system, indeed most embraced it with enthusiasm"
74	John Morahan	• A technical critique of the code and architecture reviews of the proposed system, which "contain many inaccuracies and frequently contradict themselves and each other. They reveal serious flaws in the system, and gloss over them, excuse them, or even fail to mention them entirely." Specific problems include: o insecure password protection and lack of encryption in Microsoft Access database o "virtually no exception handling anywhere in the system code" which "may well lead to the miscounting of votes" o on pseudo-randomisation for mixing votes, the seed comes of the system clock, which changes 18 times/second – "this seed may be easily reproduced by observing the exact time when the randomize function is called."

No.	*Name of person(s) or body*	*Main Points*
		• the original (vote machine generated) voter number is retained by the software even after the pseudorandom mixing of votes – this negates the entire purpose of randomising to conceal voter identity • no serious review of the Borland Delphi and TurboPower AsynchPro development environments in which the program was developed
75	Brendan Magee	• Need for an audit trail to allow the voter to be confident that the vote has been recorded correctly – citing paper copies of bank documents
76	Michael Malone	• "This Commission was formed by those who hold our fragile democracy in contempt" • "In systems of vital importance there must always be an indisputable master record that can be referred to in times of need. In this case there must be a paper record of each vote cast." • Urges Commission members to resign, given its restricted terms of reference
77	Cllr. Michael Colreavy	• People with poor eyesight and technophobes will require assistance with voting, thus compromising secrecy • Traceable paper audit trail • "Testing cannot be adequately carried out without a verifiable (by voter) parallel paper system" • Has system been field tested for effects of power outages and hardware/software failures?
78	Michael Burke	• In favour - voted electronically in Meath 2002 • But need paper trail • Need Gregory method • Need "none of the above" system • Should not limit number of candidates
79	Dr. Don Mac Auley	• Need to allow spoilt vote • "find it incomprehensible why the Government would adopt a system with no verifiable written record for such a crucial transaction" • Apprehensive about the effect of viruses and computer crashes
80	Paul Donnelly	• Cites personal correspondence with Minister and provides a number of attachments, essentially dealing with the need for a paper audit trail
81	Michael Tierney	• Cannot be assured of accuracy without publication of source code • Verification of accuracy requires parallel running of paper and electronic systems for three elections
82	Brian Mathews	Secrecy • The secrecy of postal ballots is compromised in comparison to the current system. Currently, postal votes are mixed with the

No.	*Name of person(s) or body*	*Main Points*
		others before counting. In the proposed system, someone will need to input postal votes at the count centre. When there are few postal votes for a given count centre, postal voters will have diminished secrecy of ballot • Concerns about pseudorandom storage of data on ballot module. Does the write to the ballot module have a sequence identifier? Does it have a time stamp? Is the randomizing algorithm used resistant to attack? etc. Accuracy • The chosen system is an example of a "black box" voting system – "the voter makes an entry at one side of the box and eventually a result is presented at the other side". Argues that there is no way of verifying the accuracy of a particular black box election – referring the Commission to www.blackboxvoting.com Testing: • "In any non-trivial system, testing can never verify the absence of bugs" • "No mission critical system is ever installed without a period of parallel running" – in June 2004 this will mean that there will be "absolutely no method of verifying that the results are actually correct" • "Any tests performed on software are instantly negated once an update is made to that software. The system software has been through several dozen releases" • "Therefore any claims made that the software has already been tested in the last General election are spurious. Whatever software ran then is long gone" • "If the software has required so many changes since the last general election, how accurate were the results it presented in that election?" • Field-testing in other countries is no help. "It is simply ludicrous for Government spokespersons to claim that, because one piece of software runs in one country, that a totally different piece of software will run in another country" and • System has never been tested for simultaneous multiple ballot papers – as will happen in June 2004 Conclusion "The proposed system is essentially untested and non-verifiable … the system should not be used as proposed."
83	Liam Caffrey	• Objects to system because it is a "black box" system with no voter verification • Does not support "so-called" voter verifiable audit trail because of: o Frequent printer failures o Someone smart enough to tamper with the system

No.	*Name of person(s) or body*	*Main Points*
		could outsmart the audit • Thus argues that ALL electronic systems are flawed and paper voting should be retained
84	Frank Butler	• Suggests a thorough examination of the computer program • Need paper audit trail • Has complete confidence in the Commission
85	Roscommon County Council	Resolution passed 22 March 2004: "That Roscommon County Council call on the Minister for the Environment, Heritage & Local Government, Mr. Martin Cullen, and the Commission on Electronic Voting, to ensure that no Electronic Voting takes place until a paper trail/record is put in place"
86	Frank Flanagan, Michael Ryan and Seamus Farrell	• Proponents of eventual e-voting, but not of the present system • Cite UN Covenant on Civil and Political Rights (Art. 25) – on matters such as votes being counted in the presence of the candidates, independent scrutiny of voting and counting – which they argue the chosen system will violate • Oppose use of proprietary software, given need to program complex rules and then convert these into machine code • Oppose lack of audit trail • "scant regard paid to the established methods of testing random number generators" • Advocate open source code • Advocate careful risk analysis, given impossibility of building perfect hardware and software • Advocate "two completely separate counting systems with no shared codes" • Advocate parallel running in the short term
87	Paul Holden	• Proposed system "transfers power from the ordinary citizen to the technocrat" • All software contains errors • "Business systems are typically run in parallel with manual and/or earlier functioning systems" • Voter-verifiable audit trail may be of some help, but full solution only in full paper recount, which destroys rationale for the new system • Voter-verifiable audit trail "is included in the draft IEEE Standard for Voting Equipment (IEEE Standard P1583)" – chosen system thus fails this standard • Criticises ERS tests as incomplete since ERS admit freely that they did not do an "analysis of the algorithms to the required depth" • "A system that has been subject to incomplete testing would not be used in any critical situation by responsible people"

No.	*Name of person(s) or body*	*Main Points*
88	Frank Nuttall	• Need paper trail because "I am quite sure that … people at the moment are puzzling over how to steal or alter the results…"
89	Malachy Murphy	• Software never 100% reliable • To test software, we need to match "known inputs" with "known outputs", comparing the known outputs with "expected outputs" and assuming a fault when they do not match • This cannot be done with the chosen system because there are no independent estimates of expected outputs, against which to measure known outputs • The system is therefore inappropriate
90	Celia Kehoe	• The electronic system "is far too complex for most voters to have any understanding of how it works" • There is no verifiable trail • Interference with computer data seems to be very easy to do • UN monitoring of elections insists on paper ballots • Thus need verifiable paper audit trail
91	Irish Citizens for Trustworthy Evoting	Introduction: • "Chosen system has a fundamental design flaw; it has no mechanism to verify that votes are recorded accurately in the practical setting of an election" (Abstract) • "Central to our concerns about the system is the absence of a voter-verified audit trail (VVAT)". Without this, we cannot verify the system in a way that is independent of the system itself. This lack alone "is a critical design flaw and is sufficient to render any such electronic voting system untrustworthy, and its accuracy unknowable" • Also concerned that the system has only been tested in parts, but not as a whole Section 2.1: • Statement of the need for voter verification Section 2.2: • Statement of the fact that all computer software contains bugs, and the chosen system has 220,000 lines of code written by two people • Argument that the "one giant program" approach is seriously flawed • Criticises use of Object Pascal language for a safety-critical system • Criticises use of Microsoft Access • All hardware vulnerable to malfunction • Voting machines open to tampering – most likely by reprogramming EPROM chips in machines • "Without voter verification, the system cannot be trusted to do what it is supposed to do; rather, it will do exactly what it is

No.	*Name of person(s) or body*	*Main Points*
		programmed to do, whatever that is" • Backup modules not very useful – they are only used at close of poll, and would copy any faults arising during the day • Well funded organisations have the incentive and ability to tamper • The security seals are vulnerable – and voting machines/modules must be protected 365 days/year, unlike ballot boxes Section 2.3 • Ballot modules replace ballot boxes and "it seems remarkable that in light of this major difference between the systems, more information and detail on the handling of the ballot modules is not available" • Easy to construct a device for reading a ballot module and changing its contents • Could adapt a virus to attack a Microsoft Access database Section 2.4 • Could tamper with counting software using customised virus (which would not be detected by anti-virus software) Section 2.5 • Chosen system is secret – not subject to peer review Section 3 • Votes not stored truly randomly on the ballot module • Can't cast a secret null vote • Can't convince voters that the votes are stored randomly on the ballot module Section 4: Testing • ERS estimate of 1:1000 – 1:10,000 risk not scientifically based • Nathean code review not equipped to deal with the bulk of the program – which is in Dutch. Nonetheless gave a clean bill of health to sections they may well not have understood • No test report has looked at the overall security of the system, rather than that of its component parts • System as used previously in Ireland is not the same as the system to be used in June 2004 – especially with multiple polls and new count software • No testing of machine code; there is machine code in the system that does not match the source code, and it is possible to attack a system at machine code level (undetectable in a source code review) Conclusions The bottom line argument is that there are many possible sources of failure and fraud and, however remote these possibilities are, many of them would pass undetected without independent voter verification. The proposed system manifestly does not have independent voter

No.	*Name of person(s) or body*	*Main Points*
		verification and it is therefore argued that it is unsafe to approve it
92	William Grogan	• "eVoting … is intended to get rid of paper production, storage and counting. To incorporate this into the solution is obviously ridiculous. Talk about buying a dog and barking yourself!" • Rejects right to spoil a vote, accepting Minister's argument that "the purpose of an election is to elect a government" • The flawed argument for a voter "window" to see the printed vote o The "complete flaw in this argument" is that "if someone goes to the trouble of writing a program to corrupt the vote then they will obviously have to make the program print the ballot to look the same as what the voter entered. However the corrupt program can still store a different vote in the DRE's memory. A bug could do exactly the same thing. The voter therefore is not guaranteed that what he entered is what is stored." o VVAT involves just testing a random sample – "This in itself is just another test" o VVAT involves storing the data in two places – inevitable paper and electronic votes will not tally perfectly – "paper can jam, there are small probabilities that an electronic vote will get lost". "No voting mechanism that records the votes in two places can have zero discrepancies." "What do we do then? … do we count the lot? Is the election declared null?" • "All systems are imperfect … but computer systems are orders of magnitude more accurate than manual systems" • Points to inaccuracies in the manual system – arising from miscounted votes, interpretation of ambiguous ballots, etc. • Argues that proVVAT lobby is anti eVoting • "The actual collection and counting of votes is a very trivial computer problem, far simpler than even the most basic accounts package" • Discounts most of the stories of eVoting failures as either wrong or as being in trivial elections (school boards, etc) "where security would be very light" – thus claims most stories of equipment failure are exaggerated • Criticises VVAT method in practice, mainly because of problems with printing equipment • "Academic researchers correctly point out that computer systems are not perfect … I then think they get carried away and forget that in the real world, imperfect systems must be used."
93	Tom Fennelly	• Copy of email to Taoiseach • The proposed system does not include a secure vote verification facility

No.	***Name of person(s) or body***	***Main Points***
		• This is not improved by the fact that other governments have used it • The process of testing software provides no guarantees • The only answer is a secure paper vote verification facility • "Simply making something faster doesn't constitute improvement or progress if you destroy every other quality"
94	Christopher Murray	• Support eVoting, BUT • Should have got rid of the random element in surplus distribution • Should have paper vote verification – with a parallel hand count in a random sample of constituencies • Should not modify system at this late stage to allow spoiled vote; this could not be tested • Will refuse to vote if the proposed system is used, because no guarantee vote will be correctly credited
95	Michael Monaghan	• Voter cannot verify the accuracy of the recorded vote • Many examples of hardware and software failure when eVoting used in other counties – people presumably also thought these were accurate and secret when they introduced them
96	Dr. Dervilla McKeith	• Opposes "black box" voting system • No way of verifying how a vote is recorded • No guarantee that all voting machines will work in exactly the same way • "Each voter gets a numbered ticket and the number of the ticket is entered in the register alongside the voter's name" – compromises the secrecy of the ballot • Why was no proper parallel run carried out? • What are the mechanisms for certifying any changes in the code? • Microsoft Access is not suitable for large databases – Windows not robust • Therefore need voter verifiable audit trail
97	Jason Kitcat	• Submits two papers • Author spent 3 years trying to develop a free internet voting system, before concluding electronic voting far too risky for public elections • "Voting is a uniquely difficult computer science problem because votes must be anonymous" • Malicious or accidental changes will be hard to detect • The author co-wrote and launched the European resolution for voter verifiability • The best example is the paper trail • Cites many websites on relevant matters • Concludes the chosen "black box" system should not be

No.	*Name of person(s) or body*	*Main Points*
		introduced • Second paper reports on British Electoral Commission's evaluation of pilot studies
98	Powervote Ireland Ltd.	• Their experience spans 15 years, they have accumulated a lot of knowledge in this field • Their system is used in a number of countries, millions of votes have been counted and 500,000 hours of accumulated system use have been completed successfully • The Irish implementation was subjected to significant independent tests, the results of which are available • Voters vote secretly and votes are stored randomly • Test results show the system "functions exactly as it is supposed to" • The independent test institute PTB conducted detailed tests of the voting machine • Calls for a voter verifiable paper audit trail VVPAT emanate from the USA, where different types of machine are used • The US Congress "have recently received documentation" which has examined the situation "and determines that if machines are to be used they should meet all requirements without the need to produce a VVPAT. We applaud this on the basis that … our machine does not require the use of a VVPAT to prove its accuracy" • "PTB approval was granted for this specific version of the voting machine. We are not permitted to make any changes or alterations to this without consulting PTB and our customer." • "A new version of the election management software is issued prior to each poll. A certified copy of any new version would be supplied to an independent organisation appointed by the Department" • "A major reason for the success of our system is its simplicity and ease of use" • "Microsoft and its associated Access database have been used as part of the system in Germany, France, UK and Ireland without incident" • "The source code for the voting machine and the election management software has been fully tested and approved within the project" • "Our system assures the secrecy and accuracy of the poll, if we had any doubts as an expert supplier we would withdraw"
99	Ciaran Finn	• The system does not provide any audit trail • It is inevitable that at some time in the future allegations of misuse or abuse will arise – how can these be resolved without an audit trail? • No serious risk assessment has been carried out, which is

No.	*Name of person(s) or body*	*Main Points*
		standard practice in such cases • Criticises inadequate testing for such a critical system • Argues for right to spoil vote
100	Shane Hogan	• Co-author with Robert Cochran of Labour Party submission • Must have Voter Verified Audit Trail • Necessary to check against tampering or file corruption • Alert, as in Labour Party submission, to random surplus distribution issues with VVAT, and offers solutions • Evoting must be SEEN to be accurate • Blank voters must reveal themselves, breaching secrecy of the ballot • Published voting data breaches secrecy – a person "buying" first preference votes could give each voter being bribed a distinctive "signature" sequence for their low-ranking preferences, and pay off each if this was observed in published poll data • There has been no real end-to-end testing – only testing of individual parts of the system • Randomisation feature in election management software not tested • There are no well-documented security procedures dealing with access to count centre PCs, verification of software in voting machines and count PCs, password policies, etc.
101	John Kennedy	• Need open source for all software used, including Microsoft and Borland • Need full publication for all technical specifications • These are needed to assess accuracy • Cannot test for all scenarios • Therefore proposes a specific (quite complicated) paper trail system
102	Irish Computer Society	• "..the proposed system contains a fundamental design flaw which renders it unfit for use in elections and referenda, namely that it does not incorporate any means to independently verify the results it produces" • "We have deliberately not addressed the possibility of malicious attempts to tamper with the voting system … because the provision of a means to audit election results for system error would be sufficient to detect and deter attempted fraud" • "This submission is based on a fundamental observation over more than thirty years of computing – that no amount of testing and/or review is sufficient to guarantee that any given computer system has no operational failure modes undetected by test, but discoverable in use" • Testing can show the presence of bugs, but never their absence

No.	*Name of person(s) or body*	*Main Points*
		• The chosen system has c200,000 lines of code; given industry standard figures, this implies a minimum of 10 serious system failures during the lifespan of the program • Hardware failures are inevitable – "it would be naïve to assume that computer hardware failures will always be obvious" • It may take years for some potential system failures to occur • "The conclusion is inescapable that there is every possibility that undetected error, either in the voting machines used in polling stations or those in the count centre, may erroneously affect the outcome of Irish elections and referenda, unless there is some means of independently verifying their function…. It is our contention that for these reasons, any electronic voting system must include a paper-based voter verified audit trail" • Need for random checking of constituency results with paper hand count • "After-the-fact printing of the ballots recorded electronically…is not a substitute for such an audit trail" • Problem of catastrophic failure of a ballot module in machine before this is backed up at close of poll • Problem with secret abstention Conclusions: "It is the unanimous view of the electronic voting committee of the Irish Computer Society that under no circumstances whatsoever should any electronic voting system be implemented which does not include a verified audit trail."
103	Donal Cullen	• Can design good software but, • Every computer system subject to some level of uncertainty and potential for abuse, thus • Need paper trail
104	Cllr. Austin Berry	• Will have to be shown how to use the machine and the person showing him will know how he voted • Loss of secrecy for postal ballots as these are input by someone else
105	Dr. Kevin Farrell	• Commission should have included Ombudsman and Comptroller and Auditor General • Deadline for public submissions too short – no time for FoI requests to Government • Can't judge secrecy and accuracy unless source code is public • System should be developed on open source platform such as Linux – as in Australia • Need voter verifiable paper audit trail
106	"At What Cost?"	• Cannot make full submission without source code • Need voter verifiable paper audit trail

No.	*Name of person(s) or body*	*Main Points*
		• Secrecy of spoilt/blank ballot compromised
107	Edith Wynne	• Stresses need for a paper audit trail
108	Timothy Murphy	• Not a member of ICTE, but endorses their view on voter verifiable paper audit trail
109	John Lambe	• The argument in favour of a VVAT is not that all votes need to be counted both ways, but that spot checks of voter-verified paper records are the only way to verify the accuracy of the system • States that the Irish implementation is worse than that in the Netherlands because in the latter case "each machine prints its results in the polling station after the election". The result is that tampering has to be done on a machine by machine basis, whereas in Ireland, tampering only necessary with the count computer – which is less secure, since media such as CD ROMs, USB flash drives, etc. can be inserted into it • Draws attention to a US-manufactured e-voting machine that produces a VVAT • Argues that the checks in the Irish system only amount to the system checking itself, which is not independent audit • Draws attention to the fact that votes are NOT stored completely randomly in the ballot module, cross-referencing the ICTE submission – potentially violating secrecy of the ballot • Draws attention to the fact that blank votes are not secret • The main area in this submission not considered elsewhere is an extensive review of the potential for attacks on the system – mainly with the assistance of corrupt insiders, who could be at quite a junior level • Argues that existing tests cannot convincingly deal with what would happen in the event of these attacks – since tests mainly deal with unintended faults, not intended manipulation • Argues that most of these attacks would be rendered easier to detect, and thus less likely, with a VVAT • Sets out a detailed suggestion for system for implementing a VVAT
110	Department of the Environment, Heritage and Local Government	• The product comes from a very reliable company whose reputation is excellent, and so we should expect their work in Ireland to be equally sound • The system has been adequately tested. Very extensive testing of the system has been done, by a variety of agencies and that, at some point, the testing has to stop. This point has now been reached. PTB, Nathean and ERS have all reviewed different aspects of the system, which has also been pilot tested in elections in Ireland, and in trial runs by Department officials • The new system is secure. Officials have been well trained in

No.	*Name of person(s) or body*	*Main Points*
		its use, and procedures have been laid down to safeguard the process of the election at all points. The Department points out that no officials have been involved in ballot fraud to date, and that there is no reason to expect this to start now • A VVPAT is inappropriate, as well as being costly, and has been abandoned in places (such as Brazil) that have introduced it. The key points here are: o That printers will malfunction far more often than the ballot machines will and so the voting process will be less smooth; the paper printout may also be less accurate that the electronic record o Many voters will falsely claim the paper record is inaccurate – whether for innocent or malicious reasons – and this will slow up the vote o Because currently a vote once cast cannot be deleted a VVPAT would also necessitate substantial change in the voting software to delay the saving of the vote in the ballot module until it had been validated by the voter o There would be too many requests for complete recounts using the paper ballots • The old system is not perfect. It is flawed because too many ballots were spoiled inadvertently and because of the time taken to count those preferences • Public satisfaction with electronic voting was substantial. An MRBI survey of those using the machines in the 2002 general election found that voters thought it easy to use and, by a ratio of 7:1, preferable to the paper ballot In its essentials, the case FOR the electronic voting system is that the standards set by its critics are inappropriately high and that they ignore the obvious flaws in the current system that the new system will address. The huge expense that would be required to meet demands for more expensive testing, or a VVPAT, would not be justifiable and would not improve the system at all, but might well reduce its efficiency
111	Dennis Jennings	• Argues the "absolute necessity" of a voter verified audit trail
112	Meadhbh Piskorska	• Short submission arguing that citizens have insufficient information on the proposed system to make a judgment and therefore she cannot have any confidence in it
113	David Campbell	• Argues that the accuracy of the system cannot be tested until it is made available on open source platform such as LINUX • Argues the ERS black box testing of the system cannot preclude "sleeper" viruses that will activate at a later date
114	Joe McCarthy	• One of the main arguments is that the set of tests that have been carried out are not relevant, because the system is a "moving target", with continual software upgrades – thus the

No.	*Name of person(s) or body*	*Main Points*
		"certified" system is not the actual system that would be used in June 2004. o "The Department and its reviewers do not yet have a stable version of the system" o "There is a continuous stream of releases of the election management software … After it has been stabilised how does the Department guarantee that the version of the compiled software delivered is actually the version of the source code as reviewed and tested?" • There is an argument that the Department has not deployed a well-structured and coherent testing strategy, relying on piecemeal tests of individual parts of the system, with no clearly specified test criteria • There is an argument that there is no evidence of explicit awareness in the commissioning Department of industry standard secure coding methods • On testing of voting machine, there is an argument that some results of the PTB tests were changed between the first and second reports, after consultations with the Department • On testing of the count software, the point is made that the versions tested would not be those used in June 2004 • On the source code tests, the following points are made: o Only the Ireland specific c70, 000 lines of code were reviewed, the remaining c150, 000 lines – some of it in Dutch – was not o Not all of the Irish code was reviewed because it was not available in final form at the time of the review o The manufacturers have no other client for an STV election, thus the Ireland-specific code is being written for the first time o An out of date and unsupported version of Microsoft Access (Access 97) would be used in June 2004 • Generally criticises black box testing of the count module without the source code as incomplete • Argues in detail that many of the issues raised in the Zerflow report have not in fact been addressed (including inadvertent deletion of the backup module, and the need for an audit trail) • Argues that pilots in Ireland and full elections in the Netherlands and Germany are irrelevant, since different voting machines and different software would be used in Ireland in June 2004 • States that, it would be easy to set up the chosen system as in Germany, to allow blank votes that do not force the voter to reveal his/her identity Attaches substantial supporting material, including a long list of questions to the Department, and the Department's responses

No.	*Name of person(s) or body*	*Main Points*
115	Aengus Lawlor	• From a Nice referendum e-voter, arguing that the system did not properly record spoilt votes • And raising the issue of the secrecy of blank ballots
116	Karen Devine	• Submission on the right to abstain and the right to cast a "non-of-the-above" vote, which are distinguished • A blank vote must be made known to the poll clerk who must then reset the machine, violating the secrecy of the ballot • Thus the secrecy of the casting of a blank vote is compromised
117	Edward Goroy	• Criticises Access 2000 database as insecure
118	John Fair	• Argues paper trail is essential to democracy • Suggests Lotto-like machine-readable voting slip
119	Úna Power	• Argues for paper-backed system, citing Russia, and vulnerability of Ireland to viruses/worms • Argues that non-voting electronically will be observable to poll clerk
120	Ryszard Piskorski	• Government should accept opinions of experts • Citizens need more information on e-voting
121	Ken Healy	• Poll clerks should not direct voter to use particular machine to preserve secrecy of ballot • Memory modules must be secure • Must verify 100% accuracy of counting software • Need paper printout of each vote • Preserve right to spoil vote • Need to build public confidence with expert opinions, publication of test results, opening software to independent tests, and making source code public
122	John P. Crimmins	• Strongly supports e-voting because he believes it removes need to sample votes in surplus transfers • Should randomly test system against mock paper ballots the day in advance of the election, to check against secret reprogramming in favour of some party – to enhance public confidence
123	Thomas Euferafus Griffin	• Will not vote in June 2004 because he fears tampering with the system and inaccuracy
124	Seán Dineen	• Needs paper trail, with random 4-5 constituencies also counted by hand • Need to allow spoiled votes • Should phase release of results to keep up public interest in the count
125	Mary Tierney	• Need a paper trail • Need to take more account of the needs of disabled people
126	Senator James Bannon	• Minister is Fianna Fáil Director of Elections • Negative Zerflow report • Open to manipulation

No.	***Name of person(s) or body***	***Main Points***
		• Secret source code • Need paper trail • Risk of system failure • Software continuously changing – suggesting it still has bugs • Faults may be undetectable • Potential for mistakes by voters unfamiliar with system • Pro electronic voting but not this system
127	Ferdia (as Cathair na Gaillimhe)	• Takes power from the people into the "inscrutable hands of experts" • "Utterly outraged" at financial cost – should spend money on social welfare • Computers often faulty • System can be rigged
128	James A.V. Mortell	• Need paper trail • Should use Gregory method to transfer surpluses
129	Brigid Rodriguez	• Pointless to introduce e-voting without Gregory method
130	Professor David Lorge Parnas	• Argues that much criticism/support of system is misinformed • Can trust only tests of the exact system to be used • Need to ensure design/build process conforms to that used for mission critical applications – e.g. flight control programs and nuclear power control – otherwise a problem
131	Patrick and Anne Cahill	• Current paper system secret and accurate – e-voting cannot guarantee either
132	Breeda Kelleher	• Does not trust Government not to alter results • Mistakes made every day by computer systems • Hand counting cheaper
133	Niall O'Keeffe	• Strong supporter of proposed system, which he regards as being more accurate and as secret
134	A dissatisfied voter	• Should have been sanctioned by referendum • Does not trust machines or the people who control them • Present system has no problems
135	Gertrud O'Sullivan	• Supports e-voting but this must have a paper trail
136	Brendan Atkinson	• Only the Government wants it • Britain doesn't use it • Minister is Fianna Fáil Director of Elections • Votes may go where people didn't intend them to go • Commission is a rubber stamp
137	Patrick Fagan	• Should use Gregory method
138	Bernadette Tierney	• Possible interference with code • Possible loading of votes into system • Danger of hackers • Government officials may be shareholders in the supplier company

No.	*Name of person(s) or body*	*Main Points*
139	M J Boyle	• Need parallel running of hand counted and electronic system to test it – this has not been done • Possibility of wireless hacking into system
140	Cllr. Joe Brennan	• Minister is Fianna Fáil Director of Elections • What systems will be used for postal votes? • Need for paper trail
141	Green Party/Comhaontas Glas	Secret software • Strong criticism of proprietary software. Thus the returning officer no longer has effective control over the process, which is under the control of the software developers • "It is wholly inappropriate that a private company, based outside the jurisdiction, should have this level of control over the nation's voting system" • Cites favourably the Australian Electoral Commission decision to develop and use open source software Loss of secrecy for blank ballot • Voter must make blank ballot known to voting machine operator, who must reset machine Accuracy • System only tested for tampering by "unauthorised persons" not by "authorised persons" • No security vetting of suppliers' personnel • The big issue, no independent real-time verification the system is working properly • And no ability for independent audit after the event • Only individual components of the system have been tested – there has been no end-to-end testing of the system as a whole. No testing in real life settings • Thus we need an audit trail since "it is virtually impossible to guarantee accuracy of an electronic voting system in the wild unless there is a real-time, independent, and tangible audit trail being created in parallel with the electronic systems"
142	James Cotter	• No feedback to voter proving vote recorded correctly • Previous tests not real tests because no paper verification • Problem with resetting machine on blank vote – problem of secrecy • Need to provide for spoilt votes, which are substantial in some elections/referenda • Who fixes machines on polling day – possibility of tampering then? • 2002 electronic results distorted turnout figure • e-Tallies should not be made available
143	Thomas J. Mullally	• "Fully supports" introduction of e-voting but argues for printed record of votes cast as backup against electronic failure, and very tight security

No.	***Name of person(s) or body***	***Main Points***
		• Supports because (he believes) e-voting removes random selection in surplus distribution
144	Ciaran Quinn	• No independent method for measuring accuracy of the system • Inadequate testing of system, against paper ballots, in real systems • No independent audit trail • Loss of independent monitoring by tallymen, agents, etc – the system itself is the only arbiter • "The only way for an electronic voting system to retain the advantages of a traditional paper ballot system in relation to accuracy is for the electronic system to produce a paper audit trail for the voter." • Argument about the publication of full voter preferences, and the very large number of possible permutations • Need an abstention option • Will reduce the number of polling stations (citing German evidence)
145	The Workers' Party	• Argues the fundamental need for a paper trail • Offers a Lotto-like system
146	Fine Gael Party	• Argues for an Independent Electoral Commission • Argues for a voter verified paper audit trail • Argues for publication of the program source code • Argues that the Commission should take as much time as it needs to make a decision
147	Robert McGarry	• Submits test involving asking a trained programmer to subvert the system to favour one party, and then having people vote their preferences – to see if anyone notices • Then repeat this on a national scale
148	Padraig McCarhy	• Argument for a voter verifiable paper trail, then one percent random checks on voting machines
149	F.X. O'Brien	• System open to expert tampering • Argues for the right to spoil a vote
150	Ronan O'Dwyer	• Generally opposes electronic voting • Argues for more transparency in how the system works to increase public confidence
151	Henry Byrne	• Favours the proposed system because "the activities of tallymen will be eliminated" • Argues that the Gregory method for distributing surpluses should be introduced, and that the system would be easier to validate if the random element in surplus distribution was removed
152	Niall Ó Tuathail	• "As long as the software in the voting machine is bug free there should be exact accuracy" • "The system should be tested again to try to allay the fears of doubters"

No.	*Name of person(s) or body*	*Main Points*
153	Charles Roche	• Not enough information on Commission's website to allow an ordinary citizens to assess the system
154	Paul Brennan	• Found problems with voting machine: o Buttons too small o Misalignment of buttons and candidate names o Given lighting, hard to see the number keyed in • Suggests a large monitor over the machine so that voters have a clearer idea of what they have done
155	SC	• Should check that the timing of the vote cast not recorded • Should ensure that blank voters cannot be identified • Need a lot of information about who specified, designed, built and signed off on all aspects of the system • Need to check that the software developer satisfied the Capability Maturity Model • Need to check all software resources used to build the system • Need system testing scripts used in all tests
156	The Scanlon Family	• Argues for voter verifiable paper trail • Argues for parallel running
157	William Campbell	• Argues against publication of full e-voting results because voters could be intimidated into recording a distinctive sequence of lower preferences, so that they can be identified • Believes the system probably is accurate, but that it must also be "transparently accurate" • Argues for voter verifiable paper audit trail • Argues that full system cannot be tested because of private source code of key components (e.g. Microsoft Access 97) • Example of need for voter confidence – the collapse of the FG vote in Dun Laoghaire in 2002. "The result would have undermined faith in democracy if it were not for the fact that doubters could see with their own eyes."
158	Stephen OMeara	• Stresses need for more public information on proposed system in advance of June 2004 election • Strongly objects to proposed system in the absence of paper audit trail • Questions standard of testing • Urges Commission to publish all research it does
159	Dr. David Malone	• Has written his own computer program for STV counts • Contends that the Department's document describing system is not a complete template – it needs interpretation by programmer • And stresses this is a difficult programming problem • Argues for public availability of source code – to allow independent testing • Argues checking 70,000 lines of Ireland-specific code is a "mammoth task" that "could not be done with any degree of

No.	*Name of person(s) or body*	*Main Points*
		certainty by a small number of people in a short amount of time" • Cites example of a similar important open source program in which important bugs are still being discovered • Criticises psuedo-random number generation using the system clock as a "completely discredited method" • Argues for voter verified paper audit trail
160	Micheal McMahon	• Argues: o The proposed system cannot be shown to be accurate based on testing so far o The testing needed is infeasible o The system must be modified to allow independent accuracy checks • Argues that e-voting is different from other forms of IT because the twin needs of accuracy and secrecy are to a large extent incompatible. Most checks on the accuracy of IT system violate secrecy. Most systems preserving secrecy cannot be easily verified for accuracy • Argues the proposed system sacrifices independent checks on accuracy in the name of secrecy, yet "I am not aware of any significant IT system which has absolutely no way for the user to check externally that it is functioning correctly" • Argues that PCs are insecure as it is "easy to install and replace software" • Raises lack of legal accountability of system programmers • Mounts a series of criticisms of tests to date – mainly the lack of functional checks, rather than desk checks and code reviews • Argues that "one critical function of the election management software is the collection and aggregation of ballots from ballot modules. The function was not tested • Argues that "none of the consultants' reports considers an 'end-to-end' view of the accuracy of the whole election system" • Argues that the system is highly susceptible to tampering, being based on widely available platforms such as Windows, Access, etc. "There are literally tens of thousands of programmers around the world who have the ability to write software which, once installed, would not be seen and would be highly likely to interfere with the operation of the system." • Stresses dangers of errors in subsequent releases of the software, for which testing will be less rigorous • Denies that the system facility for printing ballots is an independent check on the integrity of votes input • Denies that 15 years' successful operation is any comfort – since none of these could be verified to have produced the correct results

No.	*Name of person(s) or body*	*Main Points*
		• Argues, not for the VVPAT, but for a new system, the Chaum system, that involved voters getting encrypted ballot receipts, which they can then use to check their vote has been recorded correctly
161	Stephen G Ellis	• Argues for "printed" audit trail • Argues that system has not been tested for the entire country on one election, and that "it seems foolhardy to introduce it for two elections at once" • Argues for Electoral Commission to oversee system
162	Dr. Christophe Meudec	• Argues that an election system is a "high integrity system" for which the code needs to be proved correct using formal methods • And thus that "if the proposed software was intended to be part of an airborne system it would not have been given a certificate of airworthiness" by the FAA • Thus that the proposed system has not been tested "to a level suitable for a high integrity system"
L4	National Disability Authority	• The proposed system fails to meet many of the needs of disabled people, despite representations from the NDA following earlier demonstrations of the voting machine • Argues that many of the problems highlighted affect the secrecy of the ballot for disabled people • Stresses: o There is not independent accessibility for blind or visually impaired people o Further testing needed to assess whether the top buttons of the machine are within reach of voters in wheelchairs o Ballot and screen typefaces very small for visually impaired people o Small and inconspicuous instructions for using machine o No tactile markings on preference buttons o Reflected light affected seated voter's ability to see screen • Makes other recommendations about the conduct of the election
L5	Microsoft	Responds to criticisms of Access 97, specifically: • "while it is not recommended [to] deploy Microsoft Access for enterprise class applications, it is certainly fit for purpose for single task applications such as the chosen eVoting solution." • Nonetheless "[if] the chosen application was being written today Microsoft would be recommending the use of the latest versions of all the components that are required to build the solution" – which does not include Access but the Microsoft

No.	*Name of person(s) or body*	*Main Points*
		SQL Server Desktop Engine (MSDE) database • Argues that the reason to keep Access is that the application is already built, and works • Argues that "[if] the application developer, makes changes to the code base or underlying platform … then a full detailed verifiable systems test is required" • Agues that "this system would be viewed as 'mission-critical', but not 'enterprise class'" • Argues that Access is suitable because data is loaded onto a "stand-alone, locked down PC" • Concludes that there is "very little risk to the integrity of the vote arising from hardware failure, software failure or malicious tampering"
L16	Gerry Ellis	• Emphasises shortcomings in the proposed system, in relation to the secrecy of the vote for people with disabilities • "The proposed system is totally inaccessible to blind people. Thus they must reveal their preferences to a third party … fully accessible systems are available in the US and Europe (viz Wisekey system)" • Those who cannot use system must rely on others to cast accurate vote • Stresses need for VVPAT • Criticises use of Microsoft Access. "This is not a reliable system for such a critical system as electronic voting" • Existing limited tests are insufficient
L17	James Doorley	• Takes time to be trained to use the machine – not enough time for elderly voters • People reveal their voting choices when asking for advice on how to use machine • The forthcoming election will be more complex, with several different polls, so these risks are increased • Criticises "beep" on voting for a candidate – people outside the polling booth know how many candidates were voted for – violating secrecy • Argues for paper trail