A submission regarding accuracy and security of the chosen Nedap/Powervote electronic voting system and the testing thereof.

Dr. David Malone

March 2004

I believe that electronic voting is a step forward for our electoral system. It will eliminate a number of issues with the current system, including unclearly marked ballot papers, long recounts and particularly human errors/influences during the count.

However, I also believe that the system currently proposed can, and must, be made more secure and accurate before it goes into widespread use.

Availability of source code and the accuracy of intent

In 1998 I produced a computer program to count votes in the style of Irish PR-STV. I began by implementing the system described in the Department of Local Government and the Environment's document "Guide to the PR-STV Election System" and then refined it using the 1992 Electoral Act.

While writing this program, I became acutely aware that the 1992 Electoral Act is not a template for a computer program, it is a piece of legislation. In some cases it is unclear or ambiguous about what course of action should be taken. Even if it were completely unambiguous, the procedure for the count is tricky and not trivial to implement in a computer program.

While writing this program, I had to make choices about what I considered to be the correct algorithms. Any other programmer would have to make similar choices. However, I was conscious that programmers are not the correct people to make these choices and contacted the Department of Local Government and the Environment for guidance with respect to my implementation.

Shortly afterwards, I met Peter Greene to ask for clarification on the ambiguous areas. Peter explained that returning officers would be able to explain the existing practice, but ultimately the courts would have to decide on any ambiguous areas.

The source code for the software that performs the count in the Nedap/Powervote system is not available for examination by the courts, returning officers, candidates or the public in general. This means it is impossible for any of these people to determine if the intent of the programmer matches the legislation, and so makes it impossible to determine the accuracy of the system.

(Note that this issue of different interpretations of the legislation is mentioned in passing in one of the PMI documents.)

Availability of source code and the accuracy of implementation

In addition to the issue of the correct interpretation of the act there is the issue of bug-free implementation of this interpretation. My implementation of the PR-STV system is about 1,000 lines of code, and though I am an experienced programmer (I have been programming for about 20 years), I would not be willing to guarantee that it is entirely bug-free.

Reports of the Nedap/Powervote system suggest that there are more than 200,000 lines of code, around 70,000 of which are specific to the Irish electoral system. Finding bugs in code of this size is a mammoth task, and could not be done with any degree of certainty by a small number of people in a short amount of time.

As a comparison, consider OpenSSL, a cryptographic software library that is used to secure a large number of systems, including e-commerce and e-banking applications. OpenSSL is developed by a number of highly skilled programmers and the source code is available for public scrutiny to ensure that any bugs will be discovered and fixed as quickly as possible. Despite many careful reviews by industry experts, bugs are still occasionally discovered in the OpenSSL system, some of which are security critical.

The OpenSSL code is about 200,000 lines, and so is roughly comparable to the Nedap/Powervote system, which has not received the same level of peer review. For this reason, it is hard to believe that there are not bugs in the software that might have an impact on the accuracy of the count.

(Note that Mr. John Pugh was an important figure in both the PMI and Nathean reviews of the code, which means that this was really two phases of one review, rather than two entirely independent reviews.)

On the accuracy/security of random number generation

This issue is rather technical.

The PMI report “Evaluation of Random Number Generation in the Powervote Electronic Voting System” says in its conclusion that ‘The Delphi random number generation methodology is a perfectly acceptable solution for generating the random numbers...’. It also cautions that the ‘seed’ must not easily be reproduced, but then goes on to say that the seed is read from the clock of the system.

Choosing a ‘seed’ using a clock is a completely discredited method. This method has lead to serious security breaches in the past (for example, see the article “Randomness and the Netscape Browser” in Dr. Dobb’s Journal, January 1996). There is a body of literature on how to correctly choose a seed for a random number generator, either using more complex software methods or using special hardware.

Also, the Lehmer algorithm described is a ‘linear congruence’ random number generator. This family of random number generators are generally considered unsuitable for applications that require security.

The fact that neither of these issues was brought up in the PMI report suggests that they may not have been the right people to consider the accuracy of random number generation for this application.

On the overall accuracy of the system

Any system will only be as good as its weakest component. Even if we are sure that the software has been carefully and publicly reviewed, it is possible that something else may go amiss. Suppose the software was run on a computer with faulty hardware, such as the highly publicised ‘Pentium division bug’: would we be able to tell if the system had produced an inaccurate result?

Redundancy here is a key factor. However, a second computer based voting system is not sufficient incase it is subject to the same bug. For this reason it seems prudent to be able to fallback to our traditional counting system in the case of unexpected results and to spot-check the computer system.

Such a system could be considered as purely a check mechanism, like the tally system in place today. It need have no meaning in law, though it might naturally be considered by the courts in the event of serious discrepancies being discovered.

I hope that the Commission will consider these points when making its report. If the Commission would like further clarification, details or information about any of these points, I would be happy to respond by e-mail, post or in person.