Part 7

Summary and Conclusions

Introduction (*Part 7*)

This part summarises the Commission's work (*section 7.1*) and conclusions (*section 7.2*) in relation to various aspects of the chosen system as described in the preceding parts of this report and sets out the Commission's overall conclusion (*section 7.3*) on the secrecy, accuracy and testing of the chosen system.

7.1 Work of the Commission (*Part 2*)

Role of the Commission

The Commission's terms of reference require it to consider the secrecy and accuracy of the chosen system, to review the testing already carried out and to carry out a comparative assessment of the chosen system and the paper system of voting. The Commission has not been specifically asked to test, prove or conclusively verify the chosen system, but rather, in the context of reporting on its secrecy and accuracy, it may review the tests already carried out and carry out its own further tests.

These requirements have informed the scope and direction of the Commission's work while responsibility for policy and administration of electronic voting, including the carrying out of testing necessary to prove or verify the chosen system, remains a matter for the Government, the Department and returning officers.

Standards of Secrecy and Accuracy

Secrecy of the ballot as required by the Irish Constitution has been held by the Courts[72] to mean that the ballot is secret to the voter - "complete and inviolable secrecy" and includes the particular requirement that it must not be possible for the voter to be able to prove how they have voted. Acknowledged subsequently in sections 137 and 162 of the Electoral Act 1992, this standard of secrecy has been adopted by the Commission in its work.

Electronic processing systems can, when functioning correctly, achieve standards of accuracy that are considerably higher than the equivalent manual systems. In a critical process such as voting at national elections, it is to be expected that the highest possible standards of accuracy (i.e. closely approaching 100%) should be achieved in the electronic recording, handling and counting of votes and this is the standard of accuracy that has been adopted by the Commission in its work.

Approach to the Work

While analysis and testing of the chosen system were clearly carried out by the Manufacturers, the Department and others during the development and adaptation of the chosen system for use in Ireland prior to the appointment of the Commission, different parts of the system were reviewed by different independent bodies, both within Ireland and internationally. None of these bodies was asked to take a view of the chosen system as a whole, incorporating all relevant aspects of its

[72] *McMahon v Attorney General* [1972] IR 69, (1972) 106 ILTR 89.

hardware and software components, its physical environment and the operational arrangements for its use.

This led the Commission to take a broad view of the system within the particular scope of its terms of reference. In taking this broad view, the Commission has had regard to the key principles that any system is “more than the sum of its component parts” and is “only as strong as its weakest link”.

Software Assurance

As the chosen system relies substantially on the correct functioning of its software to achieve its purpose, a particular focus of the Commission’s work has been to investigate the quality of this software in order to determine that it can be relied upon to achieve that purpose with the requisite levels of secrecy and accuracy. Translated into software engineering terms, this requirement is expressed as assuring the “trustworthiness” or “reliability” of the software by confirming, with reference to its prescribed requirements, specifications and other indicators, that it behaves as it is intended to and that it displays no unintended behaviour.

The Commission has determined, having regard to the democratic, social and economic consequences of failure in a system that would be deployed in the critical tasks of recording and counting votes at public elections, that the standards of software engineering necessary to ensure that the overall goals of secrecy and accuracy are met by such a system are those applicable to a “mission critical” system, that is, a system in which failure can impact on the wellbeing of people who rely on it but who are not necessarily responsible for its failure.

The steps that can provide preliminary indicators regarding the reliability of the software of the chosen system have now been taken by the Commission as described in *Part 2*.

Overview of the Work

The Commission’s work programme for the purposes of this report has included work in the following areas:

- Software Assurance (*Part 3*): Investigation of the quality and reliability of the software, having regard to its defined requirements and specifications, the design and development process, the system documentation and the source code.

- Hardware Security (*Part 3*): Usability analysis and assessment of the security of the hardware components by inspection, modelling and structured analysis methods and in the context of their use at elections in Ireland.

- Testing (*Part 3*): Extension of the Commission’s previous testing of the vote counting software from 10,000 to 100,000 sample election test cases; testing of the hardware for susceptibility to hacking, electromagnetic eavesdropping or interference and power supply disruptions.

- Physical Security (*Part 4*): A "life-cycle" review of the physical and operational security arrangements for the design, development, manufacture, transport, storage, deployment and use of the chosen system.

- Comparative Assessment (*Part 5*): Identification and comparative assessment of secrecy and accuracy criteria as between the chosen system and the paper system of voting in Ireland.

- e-Voting Best Practice (*Part 6*): Evaluation of the overall implementation of electronic voting in Ireland with reference to the legal, operational and technical measures contained in the 2004 Council of Europe recommendation on electronic voting.

The full details of this work, together with the Commission's findings, conclusions and observations arising from the work are set out in the relevant parts of this report as indicated in each case above. The conclusion of each part is also reproduced in *section 7.2* below.

During the periods that preceded and followed the 10-month timeframe of the work outlined above, the Commission was fully engaged in preparatory and concluding activities concerning its work. A significant amount of this effort was directed to overcoming the constraint, identified in the Commission's earlier reports[73], whereby it had not previously been possible for the Commission to obtain access to the full source code of the chosen system, as well as other intellectual property of the Manufacturers. Moreover, it was necessary for the Commission to ensure that all aspects of its work were undertaken with due care and to a high standard.

Following completion of the Commission's work, the Manufacturers and the Department were invited to review and comment on the Commission's draft report. Where it was found appropriate or necessary, their observations on specific points have been accepted by the Commission and are incorporated in this report. Any other observations on specific points that were not accepted by the Commission or that did not require to be accommodated (being by way of commentary, additional information or clarification only) have been included at *Appendix 7* to this report.

Methodology

Persons and bodies having specialist expertise in areas including electoral law, information technology and information security were engaged by the Commission to advise and assist it in its work as provided in its terms of reference and in accordance with relevant public procurement procedures.

The Commission considered it necessary and appropriate that its work be carried out in a manner that was free from interruption, influence or interference, and accordingly determined that it would continue to meet and work in private to prepare this report as it had done for the purposes of its earlier reports.

[73] First Report of the Commission on Electronic Voting, December, 2004: Part 2 p.31.

7.2 Summary of Conclusions (*Parts 3, 4* and *5*)

This section summarises the Commission's conclusions arising from its work in relation to technical, operational and comparative aspects of the chosen system as described in the preceding parts of this report.

7.2.1 Technical Aspects and Testing (*Part 3*)

On the basis of its consideration of technical aspects and testing of the chosen system[74], as described in *Part 3*, the Commission concludes as follows:

Hardware

The main hardware components of the system, namely the voting machine, the programming/reading unit and the ballot module are of good quality and design. They are robust against failure and are well suited to their purpose. Further investigation, refinement, testing and independent certification of these components would however be necessary before they could be recommended for use at elections in Ireland. Specific areas for improvement include user access controls and device authentication measures on the voting machine and programming/reading unit and data integrity and security measures on the ballot module.

The measures implemented to secure the hardened PC on which the election management (Delphi code) software would be installed and used to configure elections and to count the votes are inadequate and would need to be reviewed and strengthened in light of the Commission's conclusion further below regarding that software.

The Commission's work has indicated improvements, many of which involve only relatively minor modifications or additions to the system, that would be necessary in order to address these issues before the main hardware components of the system can confidently be used at elections in Ireland.

Software

The embedded C code software within the voting machine and programming/reading unit is of an adequate standard and, while it is not of mission critical standard, there is evidence to suggest that it has been developed according to a recognisable structured design process that is broadly in accordance with industry best practice. Further investigation of its behaviour, followed by refinements of its functions, further testing and independent certification would be necessary before its reliability could be confirmed beyond reasonable doubt for use at elections in Ireland. Specific areas for attention include those aspects of the software that govern the user interface of the voting machine and those that govern data security measures on the programming/reading unit and ballot module. These issues can be easily addressed by modifications to the software itself.

[74] The main components of the chosen system referred to in these conclusions are illustrated for reference in *Appendix 1* and a technical description of the system is provided in *Appendix 3*.

The election management (Delphi code) software installed on the hardened PC and used to prepare elections and to aggregate and count the votes has not been developed in accordance with any recognisable standard process and is thus unlikely to be capable of meeting the high standards of software engineering that would be required in a mission critical system. Design weaknesses, including an error in the implementation of the count rules that could compromise the accuracy of an election, have been identified and these have reduced the Commission's confidence in this software.

This finding is significant in view of the critical role of the election management (Delphi code) software in configuring all of the other hardware devices and peripherals within the system at elections and its role in handling all election data, including votes. Furthermore, the fact that errors have been found in those parts of the software that have been examined and tested by the Commission raises the question of whether errors may also exist in other parts of the software that are less amenable to such examination and testing.

Given the Commission's findings about the inadequacies of the development process for the election management (Delphi code) software, and the functional errors and other weaknesses that continue to emerge it is unlikely that this software could be feasibly amended to enable its reliability to be confirmed. Accordingly, the Commission does not recommend the use of the election management (Delphi code) software at elections in Ireland but notes that it is likely that alternative election management software, compatible with the hardware and embedded C code software of the system, could be developed at a reasonable relative cost.

Peripherals

While the ballot module is robust and generally well suited to its purpose, the measures for ensuring the security of the sensitive data stored on it could be improved by the implementation of enhanced data security measures to give greater confidence in the integrity of the system.

The widespread use of CDs, in the manner currently proposed, to transfer sensitive election data, including votes, between centres is not sufficiently secure and represents a potential risk to the accuracy of elections. The use of CDs in this context and the application of appropriate security measures should be rigorously reviewed and strengthened in the light of the Commission's conclusions above in relation to the election management (Delphi code) software and the hardened PC.

The Commission has recommended data encryption and cryptographic signing of data as measures that can enhance the integrity and security of votes contained on ballot modules and CDs. Such measures can be implemented in ways that are transparent to users and operators of the chosen system and that will not impact on its simplicity or ease of use.

Security

The measures provided within the system as a whole to restrict access to its services, to enable operators and observers to check that the software and hardware versions are correct, and to protect against unauthorised access and/or alteration of data (including software and votes), are less rigorous than would be appropriate for the protection of sensitive data in a mission critical system.

There is, as a consequence, heavy reliance on the integrity of administrative procedures for the secure deployment of the system. It is desirable that greater protection against unauthorised access and interference should be afforded by the system itself in the first instance, including by means of enhanced access controls and independent software and hardware verification procedures.

These issues can also be addressed by relatively minor modifications or additions to the existing components of the chosen system.

Testing and Independent Verification

The testing of the system as a whole carried out to date, as well as the investigation, analysis and independent testing and certification of its individual components, is insufficient to provide a secure basis for the use of the system at elections in Ireland. There is thus a need for comprehensive, independent and rigorous end-to-end testing, verification and certification by a single accredited body of the entire system as proposed for use in Ireland. While the Commission’s work has laid the foundations for this process, more work will be required in this area.

7.2.2 Physical and Operational Security Aspects (*Part 4*)

The Commission recognises that success in ensuring the secure and reliable conduct of elections in Ireland to date using the paper system has been due largely to integrity and commitment on the part of the people involved at all levels of election administration. Substantial and genuine effort has also been expended and a significant amount achieved to date in many areas concerning the adoption of the chosen electronic system.

Following the assessment in *Part 4* of the physical and operational security of the chosen system by auditors appointed by the Commission, the Commission has noted the following areas for further improvement:

- the wide variation across constituencies in the proposed or actual physical and operational security measures for the management of the chosen system as a distributed system;

- the consequent need for clear policy guidance on the minimum security requirements for the custody, storage, transport, set-up, use and disposal of electronic voting equipment and data in order to bring enhanced clarity and consistency in the measures implemented across constituencies;

- the particular need for the security of voting machines to be completely assured at all times once they have been programmed for use;

- the insecurity of the methods for supplying and distributing the election management (Delphi code) software and the inadequacy of the controls on the installation, access and use of that software exclusively on the hardened PC;

- the need for enhanced data and physical security measures to be developed and implemented in the transport of votes and other election data on ballot modules and CDs;

- the need for the establishment by the Manufacturers and the Department of comprehensive electronic registers in respect of the identity, location and movement of all items of electronic voting equipment;

- the need to introduce appropriate documentary controls on the custody and movement of equipment and data, both at and between elections.

The Commission accordingly concludes that the concerns identified above will require to be adequately addressed before the overall physical and operational security associated with the manufacture, transport, storage and deployment for use of the chosen system can meet the requirements of accepted best practice.

The Commission has noted that attention to most of these physical security issues would not require any modification to the chosen system, but would nonetheless contribute very significantly to its overall security.

7.2.3 COMPARATIVE ASSESSMENT WITH PAPER VOTING (*Part 5*)

On the basis of the Commission's consideration in *Part 5* of attributes and risks as between the chosen system and the paper system, and having regard also to their relative rankings as suggested by the risk assessment carried out by the Commission, it is concluded that:

- issues of accuracy arise in relation to both systems while issues of secrecy are relatively insignificant under both systems;

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

- both systems are broadly similar in terms of secrecy and, while the chosen system can be improved to match the high standard of secrecy offered by the paper system, it is unlikely to exceed this standard;

- the achievement of the full potential of the chosen system in terms of secrecy and accuracy depends upon a number of software and hardware modifications, both major and minor, and more significantly, is dependent on the reliability of its software being adequately proven.

The Commission accordingly concludes that, when compared in terms of secrecy and accuracy, the existing paper system is moderately superior overall to the chosen electronic system as currently proposed for use in Ireland (and in some respects only marginally so). However, the Commission's work has highlighted modifications to the chosen system and the procedural arrangements for its deployment, together with further software analysis and testing of the system as a whole that could potentially remedy this situation.

The aspects of the chosen system that require modification in this respect have been highlighted specifically in *Part 5* in terms of secrecy and accuracy and in *Parts 3* and *4* as regards technical and operational aspects that have a bearing on its secrecy and accuracy. They are also reflected in the Commission's recommendations in *Part 8*.

Taking account of the ease and relative cost of making some of these modifications, the potential advantages of the chosen system, once modified in accordance with the Commission's recommendations, can make it a viable alternative to the existing paper system in terms of secrecy and accuracy.

7.3 Overall Conclusion

Based on the results of its work to date in relation to technical, procedural and comparative aspects of the chosen system, and recognising that the chosen system can potentially enhance and deliver real efficiencies in the administration of elections in Ireland (as demonstrated by systems based on the same design and used elsewhere for some years), the Commission concludes that it can recommend the voting and counting equipment for use at elections in Ireland, subject to further work it has also recommended, but that it is unable to recommend the election management software for such use.

Further work is also required in relation to the security and operational arrangements for the use of the system as a whole. The enhancement of these administrative arrangements can contribute significantly to the overall security of the chosen system without requiring any modification to the system itself.

Further development, testing and analysis of the system, followed by independent certification of its suitability are thus necessary before it can confidently be used at elections in Ireland. Desirable also in this context would be the development of Irish standards for e-voting in keeping with emerging international best practice and the assignment of responsibility to a single body within Ireland for ensuring that these standards are met.

Areas for improvement in the technical and operational aspects of the system have accordingly been highlighted by the Commission and it has made recommendations concerning the work that is necessary to address these. Approaches to further development, testing and analysis of the system have also been recommended with a view to providing the necessary assurances that the system is reliable.

Subject to this work being carried out in accordance with the recommendations of the Commission, it is likely that the chosen system can be deployed and used with confidence in the future.

In presenting its report at this time, the Commission believes that the technical and other knowledge and information about the chosen system obtained during the preparation of this report can contribute to any decisions that may be taken regarding the future development and use of electronic voting in general, and the chosen system in particular, at elections in Ireland.