

## **Part 8**

# Recommendations on the Chosen System



## Introduction (Part 8)

This part contains the Commission's recommendations arising from its work in relation to the secrecy and accuracy of the chosen system as currently proposed for use.

The findings and conclusions of earlier parts of this report are reflected and prioritised for action in these recommendations while the Commission also makes further recommendations in *Part 9* concerning alternative or complementary measures to enhance the secrecy and accuracy of the system.

## Recommendations

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

### Hardware, Software and Peripherals

- R.1:** Protections against potential vulnerabilities or weaknesses of the voting machine, programming/reading unit and ballot module identified by the Commission (*section 3.2*) should be placed beyond doubt by further independent analysis and testing of the embedded C code software (*section 3.3.1*) that governs their functions.
- R.2:** Although such use is not recommended by the Commission, any proposed use of the election management software (Delphi code) would need to be accompanied by either-
  - the implementation of additional measures to enable independent audit of its critical functions before, during and after the poll, or
  - the parallel running of another system to verify the correct operation of those functions.
- R.3:** The technical arrangements for the use of the hardened PC as a platform for administering elections should be reviewed and strengthened in view of the issues raised in *section 3.2.4*.
- R.4:** The technical arrangements for the use of CDs to transport sensitive election data (including votes in bulk) should be reviewed and strengthened in view of the issues raised in *section 3.2.5*.
- R.5:** Measures should be introduced to allow the authenticity of the hardware and software components of the system to be independently verified by operators and observers.
- R.6:** Enhanced controls should be implemented within the software and hardware to restrict access to the services of the system to authorised operators and voters.
- R.7:** Modifications to the hardware and software components of the system that are necessary to implement the above recommendations should be carried out.

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

### **Usability**

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

### **Data Security**

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

### **Physical and Operational Security**

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

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

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

**R.14:** The security of the methods for transmitting and distributing new releases of the election management software between the Manufacturers, the Department and returning officers should be reviewed and enhanced.

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

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

**R.17:** The levels of resourcing and guidance that are available to returning officers should be reviewed in light of the differences in physical security requirements between paper voting and electronic voting as highlighted by the Commission.

### **Testing and Independent Verification**

- R.18:** Verification of the entire system and the assurance of its suitability for use at elections in Ireland should be sought from a single independent body duly qualified and accredited to carry out the necessary analysis and testing activities.
- R.19:** The documented requirements and specifications of the system should be independently reviewed to ensure that they provide an adequate expression of its intended purpose and a clear description of its functions against which the system can be independently analysed and tested.
- R.20:** Following any modifications of the software and hardware components, rigorous independent analysis and end-to-end testing will be needed to confirm that the system behaves as intended and has no unintended behaviour.
- R.21:** Secure methods should be devised, in cooperation with the Manufacturers and the independent testing body, to facilitate rigorous testing of the entire system.

### **General**

These recommendations, together with the full details of the work carried out by and on behalf of the Commission should be submitted by the Department for independent technical and operational review and advice prior to implementation.

