Part 4

Physical and Operational Security Aspects of the Chosen System

4.1 Introduction (*Part 4*)

In this part, physical and operational arrangements relating to the manufacture, transportation, storage and use of the chosen system are reviewed in the light of recognised standards applicable to information security management for critical systems.

Scope of Review

As indicated in *Part 2,* the Commission considered it necessary and appropriate, in addition to reviewing the hardware and software components of the chosen system, to review also the administrative procedures and the security of the physical environment in which the system is deployed, as these can have a significant bearing on the secrecy and accuracy of the system.

In view of the distributed nature of the chosen system and its critical role in recording, translocating, aggregating and counting votes in an open public setting, with consequent reliance on the availability and correct functioning of every one of its processes, many of which remain unseen, it is essential that no perceived or actual threat to the integrity of elections should arise as a result of unauthorised access to the system at any stage before, during or after an election.

The Commission thus took a broad view in assessing the physical and operational security of the chosen system across its entire life cycle. The following life-cycle flow comprising 11 events was accordingly identified and considered as part of the review:

- Manufacture and Transport (*section 4.2.1*)
    - Design and Manufacture of Hardware and Software in Holland
    - Despatch and International Transport from Holland to Ireland
    - Local Delivery, Receipt and Functional Testing in Ireland
- Storage (*section 4.2.2*)
    - Storage by Returning Officers
- Use at Elections (*section 4.2.3*)
    - Set-up and Programming for Election
    - Transport to Polling Centres
    - Use at Polling Centres
    - Return to Storage (Voting Machine)
    - Transport of Votes
    - Read-in and Counting of Votes
    - Return to Storage and Disposal

A more detailed description of the life cycle of the chosen system is set out in the form of a process flow chart at *Appendix 4.*

The Commission also considered over-arching security aspects concerning the chosen system, including security policy management, risk assessment and asset management (*section 4.2.4*).

The work carried out is described in *section 4.2* of this part as indicated above and the Commission's findings and conclusion in relation to the security of physical and operational aspects of the chosen system are set out in *sections 4.3* and *4.4*.

Approach to Review

The Commission's review was carried out with reference to the Irish national standard on information security management systems I.S. 17799[60]. This standard provides a formal code of practice for the management of information, including electronic data and systems. It is a benchmark against which organisations can measure and demonstrate their compliance with accepted best practice in assessing risks to sensitive information, implementing security procedures to address the risks and monitoring the effectiveness of those procedures. This in turn provides confidence for the users of electronic systems that adequate measures are employed to protect against unauthorised access or disclosure of confidential information.

Each life-cycle event of the chosen system was accordingly assessed with reference to the Irish national standard. This work was carried out in the form of an audit by suitably qualified persons working on behalf of the Commission. The audit examined the controls that are implemented to restrict or prevent an unauthorised individual from gaining access to the chosen system at each stage in the life cycle and involved the following activities:

- A detailed review of documentation including material provided by the Manufacturers, the Department, returning officers and the Commission;

- Interviews with key participants in electronic voting in Ireland, including the Department, 23 returning officers, the Manufacturers, other suppliers and service providers;

- Site visits to the places of manufacture, distribution and storage of the chosen system, including 25 locations where electronic voting equipment is stored in Ireland.

In carrying out these activities, the Commission's auditors sought where possible to obtain and rely on information obtained from primary sources such as direct observation and original accounts of interviews conducted at the time of the audit. In case of variation between these accounts and other documented sources of information, the auditors relied principally on these primary sources, which describe how an activity *actually* is, or would be, undertaken in practice, rather than relying on documented formal procedures for how it *should* be undertaken. However no election was imminent at the time of the audit and it is likely the Department's advised position would be different in practice in the context of an actual election.

As no election involving use of the chosen system took place in the course of the audit, it was not possible to observe directly some key life-cycle events relating to the deployment of the system. It was however possible, in addition to interviewing all returning officers who had experience of preparing for use of the system in 2004, to interview those returning officers who did have previous experience in the actual use of the system on a trial basis in 2002.

Some of the information received by the Commission in the course of its work for the purposes of this part is confidential or may relate to the security of the manufacturing and supply processes or the security of elections. The Commission has refrained from including such information in its report of the work but this information has been taken into account in arriving at the Commission's conclusion on physical and operational security aspects of the chosen system in this part.

[60] I.S. 17799-2:2002 Information Security Management Systems – Part 2 Specification and Guidance for Use.

4.2 Review of Physical and Operational Security

This section describes the Commission's work in reviewing the security of the physical and operational arrangements implemented in the context of life-cycle events and related aspects of the proposed deployment of the chosen system.

4.2.1 MANUFACTURE AND TRANSPORT

The manufacture, transport, receipt and storage of the chosen system are illustrated as a flowchart in *Figure 2* of *Appendix 4*.

Development and Manufacture

The hardware and software of the chosen system are developed and manufactured in Holland. The voting machine, ballot module and programming/reading unit, together with embedded (C code) software, are developed, manufactured and supplied by Nedap N.V. at Groenlo and Eibergen. The election management software supplied in Ireland by Powervote Ireland Ltd. is developed and maintained by a third party software developer, also in Holland.

Nedap N.V.

Auditors appointed by the Commission visited the premises of Nedap N.V. at Groenlo and Eibergen to assess the physical security surrounding the development and manufacturing processes of the voting machine, ballot module and programming/reading unit, together with the embedded (C code) software.

The physical security measures surrounding the development and manufacturing processes were fully examined on behalf of the Commission. Access controls and other physical security measures and procedures were identified and evaluated.

The hardware manufacturing process was found to be substantially self-sufficient with most component parts of the electronic voting equipment being manufactured and assembled in-house. Within this process there is only a limited reliance on third-party suppliers for the provision of a small number of standard component parts. Details of these suppliers were also seen and reviewed on behalf of the Commission. No critical dependence on any supplier was identified. Component parts are procured or manufactured directly to meet production demand and finished products are manufactured and supplied to order, so there is accordingly no bulk storage of component parts or finished voting equipment.

Research and development activity associated with the development of the hardware and embedded (C code) software of the chosen system is carried out in a secure electronic systems research and development area under the full control and ownership of the company, which also owns the intellectual property vested in the products. Encoding of proprietary firmware onto hardware devices is carried out under special security procedures at the assembly line, although these procedures were not observed.

Finished products are dispatched for delivery by accredited carriers in containers loaded directly from a secured area within the manufacturing site. Details of this process are outlined further below.

Overall, while the development and manufacturing facility has not been certified for compliance with national or international standards such as ISO 17799/27001, it was clear that considerable effort had been expended by management to control and monitor the movements of personnel within the facility and to restrict unauthorised access and, in particular, to monitor and restrict access in secure areas of the facility. There is a strategy for ensuring continuity of service in the supply and maintenance of company products in general, although this is not specific to its Irish electronic voting products. This strategy includes disaster recovery planning and the division of job skills among staff to ensure production capability. It was also noted that there is a management commitment to instilling a company culture that recognises and protects the sensitivity of information and materials handled by employees.

While there is currently no supply dependency in the provision of component parts or any other single point of failure that might interfere with Nedap's ability to manufacture or maintain voting equipment in Ireland, it was recognised that the use of the Nedap components of the system in Ireland is critically dependent on the election management software supplied by Powervote Ireland Ltd.

Powervote Ireland Ltd.

Powervote Ireland Ltd. has supplied an election management (Delphi code) software product that can be used in conjunction with Nedap hardware and software to manage the organisation and conduct of elections. This product has been developed by a third party software developer and adapted by them for use at Irish elections. No other parties have rights to the source code associated with the Irish implementation of the software.

Through communications with Powervote Ireland Ltd. on behalf of the third party software developer, the Commission's auditors assessed the physical security measures surrounding the development of the software. Access controls and other physical and logical security measures were identified and evaluated and evidence was sought of the existence of documented development and change control procedures.

International Transport and Local Distribution

Hardware and Embedded Software

The hardware (voting machines, ballot modules and programming/reading units) and the embedded C code software of the chosen system are transported from Holland to Ireland, typically in bulk consignments. The following description relates to the arrangements implemented for the original supply, in a number of separate bulk consignments, of the voting equipment necessary to conduct a national election. Subsequent to this, voting equipment has also been transported between Holland and Ireland for modification, analysis or repair by similar means, either in bulk or in smaller quantities.

As indicated further above, finished manufactured products are dispatched for transport by road and sea in containers loaded directly from a secured area within the manufacturing site in Holland.

Containers are loaded and sealed conventionally according to standard container freight arrangements before being transported by road to a shipping port where they are transferred to a cargo vessel by crane as load on/load off freight for onward transportation by sea to Ireland. Prior to loading, the container seals are checked by a port agent. Storage arrangements in Holland prior to sea transport are in accordance with TAPA (Technology Asset Protection Association) requirements.

Receipt of the containers in Ireland and onward distribution of their contents is handled by an Irish freight company who check the container seals before removing the container to their premises where it is opened and its contents distributed into vehicles, according to consignment instructions, for delivery to individual returning officers at locations throughout Ireland.

Functional testing of the equipment is carried out by returning officers before documentation acknowledging receipt is returned to the Manufacturers and the equipment is placed in storage locally.

The containers and road transport vehicles are provided by freight companies in Holland and Ireland and the overall transport arrangements, including the selection of the freight companies and the sea carrier, are coordinated by a shipping agency in Holland engaged by the Manufacturers.

A communications and documentation trail is kept in respect of the equipment during transportation which gives visibility on progress and on any problems arising while in transit and records are maintained by the Manufacturers to account for the delivery of all equipment in Ireland.

Security aspects of the despatch, transport and delivery processes outlined above, including as regards any intermediate storage requirement arising during transit, were identified and reviewed by the Commission’s auditors. However no transport event was observed during the audit.

Hardened PCs and Related Peripherals

The hardened PCs were manufactured by Hewlett Packard in France to a standard specification and supplied in Ireland, together with printers, by an Irish technology company contracted by the Local Government Computer Services Board, acting on behalf of the Department. A second Irish technology company was contracted by the first technology company to undertake the PC configuration “hardening” process at a secure facility in Dublin before the PCs and printers were delivered by road to returning officers for storage. Receipt was acknowledged by the returning officers but functional testing was not required. Smart cards used to access the services of the PCs were distributed to returning officers by registered post.

The Commission’s auditors identified and reviewed the arrangements for supply, hardening and distribution of the hardened PCs as described above, including by an audit of the premises at which the hardening process was carried out. However no such event was observed during the audit.

Election Management Software

Election management (Delphi code) software is sent by the Manufacturers from Holland to Ireland either on CD-ROM transmitted by post or by e-mail addressed to either the Department or the Local Government Computer Services Board acting on behalf of the Department.

Onward transmission of the software to returning officers was effected originally through the hardening process applied to the PCs as described above. During this process the software was installed onto each PC as part of a standard software configuration determined by the Local Government Computer Services Board acting on behalf of the Department.

Subsequent updates of the software received from the Manufacturers have been disseminated on CD-ROM by post to returning officers who have then loaded the software onto the hardened PCs.

The Commission’s auditors identified and reviewed the arrangements for supply of the election management software as described above.

4.2.2 STORAGE

Voting equipment hardware and software is stored at 25 storage facilities procured locally by individual Dáil constituency returning officers throughout Ireland. Equipment is also stored by the Department of the Environment, Heritage and Local Government in Dublin.

Site visits to each storage location were carried out by the Commission's auditors in order to assess the physical security and related arrangements implemented to protect the equipment from interference or damage resulting from unauthorised access or inappropriate storage arrangements.

Storage Between Elections

Each storage location was surveyed using a layered approach to identify the physical characteristics of the location and its surrounding environment as well as the functional measures in place to deter, delay, detect and respond to any unauthorised access. The measures taken to protect the equipment from environmental conditions were also examined in the light of specific guidance provided by the Manufacturers and in the light of best practice for the management and use of electronic equipment. This approach is summarised in the following paragraphs and a fully detailed report on the security of each location was provided to the Commission as a result of this assessment. These reports have been taken into account by the Commission in its findings and conclusion on physical and operational security aspects of the chosen system.

Environmental Surroundings

Consideration was given to whether a storage facility is surrounded by urban, residential, industrial or rural areas; the particular security characteristics, advantages and disadvantages of each type of area; and the existence of any knowledge or other information (including media reports concerning storage arrangements) that might disclose either the location of the facility or the fact that it contains electronic voting equipment.

Immediate Surroundings

The site and perimeters immediately surrounding the storage facility were considered as respects the provision and effectiveness of boundary walls, fencing and gates; the levels of supervision provided and the levels of public access allowed at different times of day; the contents, uses and other activities associated with adjacent premises; and the extent to which the use of an equipment storage facility is shared with other activities.

Building Perimeters

The fabric and construction method of the building structure was considered (e.g. stone-built cellar, brick walls, tiled or metal roofs, etc.) but excluding access points within the structure which were considered separately.

Building Access Points

Principal access points including windows, pedestrian entry/exit doors, vehicle and goods entry/exit doors and skylights were considered, as the measures taken at these points can contribute to the deterrence, prevention and delay of unauthorised access. The location and accessibility of doors, windows and frames and the provision of shutters, barriers, crash-bars, and grilles of suitable strength were reviewed together with the use of adequate locks, keypads and other access controls. Access points require particular attention as they are sometimes considered in isolation from each other, thus contributing to possible inequality of security protection across access points within a building.

Detection, Delay and Response

Assuring complete deterrence or prevention of entry or attempted entry to storage locations by unauthorised persons is not feasible in most prevailing circumstances where it is necessary to store voting equipment. Consideration was thus given to measures for the detection of unauthorised access and the provision of response, as detection is of little use without the ability to respond appropriately. Significant also in this context is the provision of delaying measures to allow a sufficient interval for a response to be provided between the detection of entry to a facility and the gaining of access to voting equipment. Measures considered included the provision, testing, monitoring, triggering and quality of implementation of alarms and other monitoring systems such as CCTV and security personnel, the levels and methods of response, planned response times, the "layering" of detection measures to mitigate any failures and the strategic location of equipment (and equipment of varying value or sensitivity) within and between storage locations.

Other Considerations

In addition to the above, the Commission's auditors considered the provision of smoke detection devices, anti-dust coatings on floors and walls and, where storage locations are also used to set up equipment for use at elections, the provision of appropriate electrical outlets, centrally located, to avoid trailing cables and to facilitate safe access and movement by staff around the equipment.

Temperature and humidity tolerances of the voting equipment have been specified by the Manufacturers and it was noted that most returning officers have implemented storage heating and some have also implemented humidity controls to meet these requirements.

Wheeled trolleys are provided for the storage and transport of a number of voting machines together and dust covers are also available but are not supplied in all cases. Ballot modules are stored and transported to and from storage in metal cases lined with slotted protective foam inserts, although the foam inserts were not present in all cases.

The storage of hardened PCs, the related smart card access controls and copies of the election management software on CD was also specifically reviewed in the context of the segregation of key components of the chosen system and the particular security requirements associated with each component.

Storage and Custody During Elections

Voting equipment is always potentially vulnerable to unauthorised interference, whether targeted at denial of service or at altering its behaviour. Special attention to the security of voting equipment is therefore warranted at election times because, once prepared for use, the equipment is at its most sensitive and additional potential vulnerabilities arise in respect of ensuring its correct configuration and preventing the unauthorised entry of votes or subsequent interference with votes cast validly.

Although electronic voting has previously been implemented at elections and referenda by only two returning officers and in a small number of constituencies, most returning officers interviewed by the Commission's auditors had prepared plans for use of the chosen system in all constituencies, as proposed for the European and local elections in June 2004. These plans varied in terms of the additional security measures that would be implemented in respect of electronic voting equipment at election time and some were dependent on the availability of Garda personnel or the provision of adequate funding for the hire of other security personnel.

Following the programming of ballot modules and the testing and configuration of voting machines in the days immediately before an election (already described in *sections 3.2.1* and *3.2.2* of *Part 3*), the following options have been considered by returning officers for custody of voting machines until they are used on polling day:

- Retain voting machines overnight at main storage location, in some cases under guard, until they are collected by, or distributed to, presiding officers on polling day;

- Transport voting machines to distributed storage locations within constituency and retain overnight, in some cases under guard, until they are collected by, or distributed to, presiding officers on polling day;

- Voting machines distributed or collected immediately following programming and retained overnight in custody of individual presiding officers;

- Voting machines distributed or collected immediately following programming and retained overnight at polling centres, in some cases under guard.

Almost all returning officers recognised that a programmed voting machine is more sensitive than one that has yet to be programmed. However, not all of the various proposed arrangements for custody and storage of programmed voting machines indicated a clear appreciation of the essential and fundamental difference between the former ballot box under paper voting and the voting machine as an electronic ballot box under the chosen system.

Once programmed, each voting machine has the combined sensitivity of an empty ballot box and a number of blank ballot papers. While the same sensitivity also exists under the paper system, segregation of empty ballot boxes and blank ballot papers (usually locked within one or two ballot boxes until the day of the election) is more easily achieved and proven. There are also additional sensitivities of the programmed voting machine and its configuration that do not exist under the paper system.

For these reasons, the former practice whereby a presiding officer could receive the ballot papers for a polling centre on the evening before the poll and retain them in close personal custody overnight (in one or more sealed ballot boxes), while leaving the empty ballot boxes unattended at the polling centre, would be inadequate to protect programmed voting machines under the chosen system. While it would be physically impossible for a single presiding officer to transport or exercise close personal custody over the number of voting machines required at many polling centres, it would equally be inappropriate to leave the voting machines unattended at polling centres overnight.

Although it would be preferable to deliver voting machines directly from storage to polling centres on the morning of polling day, it is necessary to programme and distribute voting machines not later than the evening before in order to facilitate earlier opening of polling centres, to avoid delays in setting up the equipment on polling day and for other logistical reasons of distribution within constituencies. The introduction of the chosen system thus entails an additional requirement for the security of voting machines to be completely assured at all times once they have been programmed for use[61]. This requirement applies equally after they have been used and until the election has been completed (as discussed below).

Health and safety requirements also apply for staff who must handle voting equipment at elections. Some guidance and training has been given in lifting and setting up the voting machines which requires two persons. As these are the most numerous and widely distributed components within the chosen system, many presiding officers will require additional assistance and some returning officers have arranged for such assistance to be provided. The handling and set-up of programming/reading units and hardened PCs is a lesser concern as these are smaller, lighter, easier to handle and are used only at fewer, and more centralised locations.

[61] The Department has separately advised the Commission of the following specific procedures concerning the security of voting machines after they have been programmed for use:

- once the programmed ballot module is placed in the voting machine, a seal with a uniquely numbered serial number is attached to the lock that holds the ballot module in place;
- a second seal is placed outside the voting machine after it has been checked and closed;
- both seals are checked, as part of the open poll procedure, prior to the voting machine being used for voting and the presiding officer must verify that the serial numbers on the seals match those listed in the accompanying paperwork;
- if there is any doubt as to the integrity of a voting machine prior to use, it is taken out of service and a spare machine replaces it.

4.2.3 USE AT ELECTIONS

Security aspects of the use of the chosen system at elections were also considered on the basis of a review of the documented guidelines issued to returning officers by the Department and the Manufacturers and also on the basis of interviews with each returning officer carried out by the Commission's auditors.

Additional information was received subsequently from the Department indicating that the Department's advised position was different from what had been indicated by the Commission's audit. The Department has further indicated that these matters would be addressed and that appropriate guidance would be given in advance of any election.

Set-up and Programming for Election

It was generally reported by returning officers that the programming of ballot modules and the testing and configuration of voting machines immediately prior to an election would take place at the long-term storage facilities described above. This process is illustrated as a flowchart in *Figure 3* of *Appendix 4* and further descriptions of the process are given in *section 3.2* of *Part 3*. The general security considerations surrounding the storage of the voting machine, once configured for use have been outlined in the previous section in relation to storage.

The set-up process concerning the use of the hardened PC to set up the election data and the use of the programming/reading unit to programme data onto the ballot modules was also identified and considered by the Commission's auditors. In some cases, these activities (described in *section 3.2* of *Part 3*) may take place at the election office of the returning officer and the programmed ballot modules are then transported to the storage site where they are inserted into voting machines.

- It was observed that the security and other measures implemented in respect of the hardened PC could be bypassed simply by installing and running the election management software on any other PC, thus undermining the protections intended to be provided by the hardening process.

- Version and distribution control of the election management software were not well implemented and were not implemented on a centralised basis.

- There appeared to be no procedure or guidance governing the functional testing, use, storage, re-use, upgrading and re-versioning of the hardened PC and its software.

- Storage of the hardened PC, election management software and related peripherals between elections took place in most cases at the offices of returning officers where they may be susceptible to greater day-to-day risk than if they were kept in a dedicated storage facility.

- There was not absolute clarity among returning officers concerning the alternative uses that the hardened PC could be put to between elections and also as to whether a new PC would be provided for each election or how its hardening and anti-virus measures would be upgraded prior to each use.

- The proposed use of CDs to transmit candidate and related election information, including votes, between Dáil (service level) returning officers and other returning officers at various stages before and after a poll was noted.

- Although, at an operational level, any interception and/or tampering with data transmitted on CDs should be detected by procedural checks before the election, the interception or loss of a CD could at least cause embarrassment or inconvenience in the set-up process and, accordingly, increased physical and data security measures should be applied as outlined further below in relation to the transport of votes on ballot modules and CDs.

It was generally noted that work was in progress on many of these matters at the time of the proposed first use of the chosen system on a nationwide basis in 2004 and that this work had not been completed at the time of the audit carried out on behalf of the Commission in 2005.

Transport to Polling Centres

The general security considerations surrounding the transport of programmed voting machines to polling centres have been outlined in the previous section in relation to storage. It was observed that the proposed transport arrangements vary greatly between returning officers. As indicated previously, these arrangements can include delivery to the polling centre or collection by the presiding officer from the storage facility either on or before polling day. In other cases, regional distribution centres within constituencies were proposed.

In the case of delivery, this was typically proposed to be arranged through the same carrier, courier or taxi services used previously for the delivery of ballot boxes and paper ballots as these had been found by returning officers to be trustworthy and reliable under paper voting. While this approach may offer the comfort of familiarity and consistency of dealing with the same company as under previous arrangements, it is likely, given the relative infrequency of elections, that many of the individual drivers involved would not have had previous experience of the delivery process.

The Commission’s auditors found only one case where it was proposed that drivers should produce identification as a prerequisite to collecting voting machines and in no case was it proposed to have a specific security presence accompanying the machines while in transit. No specific instructions regarding security were given to personnel involved in transport and mainly geographical rather than security considerations appeared to have been taken into account in planning delivery routes. Although many constituencies proposed roaming supervisors who would have spare voting machines if required during polling day, there were no specific continuity arrangements in the event of a breakdown or accident involving a transportation vehicle.

Procedures for the delivery of voting machines at polling centres also varied considerably. In some constituencies it was provided that a Garda should sign an acceptance sheet at the polling centre and delivery was not to be effected unless a Garda was present. In other cases, voting machines would be delivered and left unattended at the polling centre on the assumption that the polling centre would be locked until other staff arrived to assemble the equipment. In most cases delivery was planned to take place the night before polling day and assembly would take place on the morning of polling day. In many cases however, formal signed receipt of delivery was not required and it was acknowledged that if the designated recipient was not present or if the polling centre was locked at the time of delivery it was possible that a delivery would be left in a location at or near the polling centre.

It was also proposed in some cases that individual presiding officers would collect voting machines and store them overnight at their own discretion as regards security. It was uncertain whether it was acceptable to leave a voting machine overnight in a locked car but concern was certainly expressed at the health and safety implications of requiring presiding officers to lift heavy equipment into and out of their cars for overnight storage indoors.

In general, the Commission's auditors observed that many returning officers referenced previous arrangements for the transportation of ballot boxes and ballot papers under paper voting and anticipated that the same or similar arrangements would apply in the case of electronic voting machines.

Use at Polling Centres

The process for the set-up of voting machines at polling centres, their use by voters and the close of poll is illustrated as a flowchart in *Figures 4* and *5* of *Appendix 4*. A further description of this process is given in *section 3.2* of *Part 3*.

The security risks associated with the use of voting machines once set up at polling centres were found by the Commission's auditors to be quite low, since the continuous presence of the presiding officer and polling clerks means that the equipment can be fully overseen at all stages other than when it is being used by voters. It was considered that the likelihood of deliberate damage or sabotage in this context was also quite low. However, a number of other issues arose:

- confidentiality or non-disclosure agreements can be used to give notice and reinforce the understanding that election information is confidential or secret: however no such measures appear to be included in the terms on which polling staff are engaged;

- it is important that adequate training should be provided to polling staff on security procedures and the correct use of voting equipment: given the relative infrequency of elections, such training would need to be repeated in advance of each use of the equipment;

- voting equipment and related devices and media should never be left unattended in public places;

- the adequacy of insurance to cover voting equipment while in use should be confirmed;

- the weight of the tables used to hold voting machines while they are in use makes them difficult to move, a lip at the back of the tables requires that voting machines be opened and assembled before they are placed on the tables, and the tilt mechanism provided for special needs voters makes the tables unstable with potential for injury to voters or damage to the equipment.

Return to Storage (Voting Machine)

It was found to be the generally accepted view among returning officers that the sensitivity of the voting machines diminished greatly once the ballot modules containing the votes were removed following the close of poll and sent for read-in, aggregation and counting.

In some constituencies it was intended that voting machines would be left at polling centres until collected and returned to storage the following day. It was not anticipated that any specific security measures or physical presence would be provided during this period. In other cases it was intended that the voting machines would be collected and returned to storage on the evening of polling day.

Likewise, where voting machines had been collected from storage by a presiding officer, it was expected that the same procedure would apply in reverse, either on the evening of polling day or on the following day.

In only one case was it observed that staff involved in the collection of voting machines would have to identify themselves or carry formal paperwork and it was generally not observed that voting machines should be accompanied by custody documents to be signed over to the transport staff or agency or governed by a manifest detailing the machines to be collected.

As each voting machine contains a backup ballot module which becomes the primary record of the votes cast on that machine in the event of any failure or loss of the primary ballot module, it is necessary that the security arrangements surrounding the backup ballot module are no less than those surrounding the primary ballot module until such time as the votes have been secured centrally.

In one case it was suggested that all voting machines might be transported to the read-in centre together with the ballot modules. This would be both impractical for logistical reasons and inadvisable for security reasons as the benefits of retaining a separate backup of the votes would be diminished by transporting both the original and the copy together.

It was indicated subsequently by the Department that the advice that would be given to returning officers was that a poll official should remain with the voting machine up to the point where it had been confirmed that the primary ballot module had been successfully read in for counting.

It would also be important however, in case of any subsequent review of the election, to be able to confirm that a voting machine was not capable of being interfered with or altered in any way following the poll so that it can, if necessary, be preserved and examined in exactly the same condition as it was used by voters during the poll.

Transport of Votes on Ballot Modules and CD

Depending on the number and type of elections being held together, votes on ballot modules may either be transported to read-in centres in the first instance, before being transferred to CD and transmitted onwards to various count centres, or they may be transported directly to count centres where they are read in and counted.

Votes on Ballot Modules

It was recognised by returning officers that the ballot module containing the votes cast is at least as sensitive during transportation after the poll as the programmed voting machine prior to the poll.

Although the Commission’s auditors observed that frequent reference is made to the secure transportation of ballot modules, there appears to be no clear definition of what this means. In some cases, secure transportation was understood to include delivery by a taxi company or courier, in other cases delivery by at least two nominated poll staff was envisaged while in other cases secure transport required that poll staff were to be accompanied by a Garda escort.

While all returning officers recognised there was a need for two persons to be involved – one to collect the ballot modules at each polling centre while another remained in a vehicle with the ballot modules already collected, it was not observed in any case that there was a requirement for collection staff to verify their identity to polling centre staff.

In general it was anticipated that the ballot modules, together with associated voting machine print-outs, signed forms and stub books would be placed in a jiffy bag or similar package for transport. The proposed use of sealed or tamper-proof containers for this purpose was not observed.

The availability and authenticity of ballot modules as critical devices within the chosen system has a very high profile. Any incident that occurs during the transfer of votes on from polling centres or which comes to light on their receipt at read-in and count centres will thus be obvious to observers and has the potential to influence confidence in the chosen system.

Votes on CDs

In addition to the distributed nature of the voting machines and ballot modules used to record and gather the votes, the equipment used to aggregate and disaggregate votes for different elections and to transfer them to the relevant count centres is also of a distributed nature as described in *section 3.2* of *Part 3*. Once the votes read in from ballot modules at read-in centres and at Dáil (service level) count centres have been aggregated into files relating to each election, they are then copied from the election management software onto CDs and transmitted to the relevant European and local count centres, where they are imported into a separate installation of the election management software for further aggregation and/or counting by the relevant European or local returning officer. (The totals of votes aggregated and counted locally at the service level in respect of Presidential elections and referenda are relayed by fax and telephone to a single national returning officer.)

At a national poll involving elections of different types, there would be a significant number of CDs in transit between various read-in centres, service centres and count centres. As this procedure currently stands, it was observed that it may be possible for someone with access to a copy of the election management software to prepare and substitute an alternative CD containing a bogus set of votes or to intercept the official CD and alter the votes recorded on it. It was noted that, unlike in the case of altering or substituting a ballot module, no special hardware would be required to carry out such an attack, apart from the provision of a substitute CD of authentic appearance.

Significant also is the fact that the numbers of votes transported on each CD will be far greater than those contained on a single ballot module. Although any votes that are lost or corrupted as a result of such an attack can be recovered from the primary or backup ballot modules or from within the election management software (provided the interference is detected by administrative procedures), the interception, substitution, alteration or loss of a CD has the potential to affect confidence in the system as a whole.

At the time of the first proposed nationwide use of the chosen system at local and European elections in 2004, work was in progress to develop and implement security measures in respect of CDs. These included saving vote files in XML format and with the vote data encrypted prior to copying to write-once only type CDs, providing outer identifying labels and recording serial numbers and other identifying information on the front of CDs, authentication by returning officers' signatures and the provision of paper copies of data to accompany the CDs.

Additional protections that could be considered in this context would include the application of security measures to the data such as enhanced encryption to prevent unauthorised reading of the data and cryptographic signing to protect against unauthorised access and malicious or accidental alteration of the data. The protections should in any case be no less than those applied in the case of ballot modules.

Technical issues associated with the secure use of ballot modules and CDs under the chosen system are addressed in *Part 3* of this report.

Read-in and Counting of Votes

The process for the read-in and counting of votes is illustrated as a flowchart in *Figure 6* of *Appendix 4* and a further description of this process is given in *section 3.2* of *Part 3*.

The receipt and movement of vote data to, from and within read-in centres, service centres and count centres provides further potential opportunities for the accidental or deliberate substitution, alteration, loss or destruction of votes. While all returning officers agreed that the physical security of the voting equipment at these centres should be high, it would also be desirable that specific guidelines be issued to provide a common standard to be implemented across all centres.

Within the timeframe of the Commission's work, no election took place at which the Commission's auditors could observe the security measures implemented. However, from the review of guidelines already issued by the Department and from interviews with returning officers, guidelines should include the following:

- clear definition of security perimeter and use of barriers and signage to segregate public areas from staff areas;

- provision of a manned reception area or other means of controlling physical access to the centre;

- orientation and positioning of computer screens and other equipment to limit unauthorised observation of information prior to official announcements (but while maintaining appropriate levels of transparency and observation in the administration process);

- additional measures such as the use of password protected screen savers, enhanced swipe card access and the maintenance of a clean desk policy when it is necessary to leave a workstation unattended;

- requirement for personnel to wear visible identification and to be encouraged to challenge strangers and anyone not wearing identification;

- prohibition of eating or drinking in proximity to information processing facilities.

Variations were observed in the proposed arrangements for the incorporation into the electronic count of the votes cast on paper by postal and special voters (which entails the individual re-recording of these votes into voting machines by poll staff). These variations related to which, and how many, staff should enter and check the votes, how and when this should be carried out and the levels of oversight and verification that should be implemented to ensure the accuracy of the process. A standardised procedure is thus also required in this area.

Technical issues associated with the secure use of the hardware and software of the chosen system in a public setting are addressed in *Part 3* of this report.

Return to Storage and Disposal

It is also important to ensure the secure custody and/or disposal of media and equipment containing used data after an election. Examples of such items in the chosen system include the following:

- votes on ballot modules,
- votes on backup ballot modules,
- votes on CDs,
- votes on count PCs,
- printouts of individual votes,
- tables and intermediate tables of counted votes on PCs,
- printouts of tables and intermediate tables of counted votes,
- licensed proprietary software stored on voting equipment.

It is necessary that all items of equipment and storage media be considered to ensure that any sensitive data or licensed software is handled appropriately following an election. Damaged items should be assessed for repair or destruction while the disposal or deletion of all sensitive items should be logged for audit purposes.

There is a specific statutory requirement that paper ballots be retained for six months after an election and that they should then be destroyed. As individual ballot modules can contain votes relating to different elections, and as the requirement to retain votes for 6 months may involve different custodians in respect of votes of different types, some lack of clarity was observed by the Commission’s auditors regarding who should retain ballot modules in these different circumstances.

Additionally, and unlike the paper election process, the electronic voting process contains multiple copies of individual votes (as indicated above) and consideration needs to be given to which and how many of these copies need to be erased or destroyed in order to meet the statutory requirement for destruction of the ballots.

4.2.4 Security Policy Management

Knowledge and Training

It was observed by the Commission's auditors that, while there is liaison between returning officers in relation to the election responsibilities they share in common, and while guidance has been provided by the Department to all returning officers, it is a significant characteristic of the administration of elections in Ireland that each returning officer operates essentially alone in the discharge of his or her electoral responsibilities.

This means that each returning officer has individual responsibility for the selection of staff, budgeting and finance and for the procurement of premises, goods and services necessary to run an election in their constituency, as well as the implementation of statutory requirements, Department guidelines, other applicable measures and measures of best practice in a wide number of areas, including security.

There is clear evidence that each returning officer views security as a significant issue and has attempted to implement what he or she sees as the most appropriate security controls. Most have made efforts to obtain insights into security planning and some have obtained specialist advice. However none have received specific guidance or training on security. As a result, all returning officers are implementing controls in isolation while some are equipped with little knowledge of what equates to best practice. Notwithstanding this, returning officers in some constituencies have been highly innovative in their approach to ensuring the security of the electronic voting equipment. Although these returning officers have identified and met the requirements of best practice and have achieved very impressive results, there is no formal mechanism for others to learn or benefit from this experience.

There is thus a need for centrally coordinated guidance and training in security principles and for a collective pooling of experiences across all constituencies in order to facilitate the identification and documentation of specific security requirements, controls and procedures covering all aspects of the management and use of electronic voting equipment.

Other Cross-Cutting Issues

Other aspects of the administration of elections across all constituencies that can have a significant bearing on the security requirements of the electronic voting system were also noted by the Commission's auditors and these are recorded below.

Selection and Training of Staff, etc.

The effective administration of elections in Ireland under the paper system of voting implemented to date has relied significantly on the quality and integrity of the personnel selected by returning officers to act as election staff. Experience suggests that the approaches taken to date in the appointment of staff have been successful and, consequently, that there is a high level of public trust in Irish election officials at all levels to ensure the continued secrecy and accuracy of elections.

The proposed introduction of electronic voting generally, including under the chosen system as proposed for Ireland, brings new challenges to the maintenance of these high standards in the administration of elections since there is considerably reduced transparency in the administration process generally under electronic voting, while the electronic vote itself is susceptible to new and additional risks that are not present (or are present in different measure) under paper voting. Some of these risks lie beyond the immediate control of election staff themselves, while others arise from the possibility of deliberate or inadvertent staff error in handling the electronic system.

Under electronic voting, there is a requirement for returning officers to satisfy themselves that their staff and any third parties involved in the provision of services at the boundaries of the system comply with more rigorous standards of personal suitability and security awareness, in order to ensure appropriate levels of security in the overall deployment of the system. This may require the security vetting of third-party service personnel and companies, as well as persons appointed directly by returning officers, and also the provision of training to enhance security awareness among election staff as a whole.

In addition to training on security aspects of the system, it will also be important for staff to be fully trained and re-trained in advance of each election on the technical operation and use of the chosen system, so that the learning experience from each use of the system can be reinforced and enhanced.

A further consideration in this context is the rotation and segregation of staff responsibilities so that there is a reduced likelihood that key knowledge and responsibilities are vested in only a few personnel at successive elections, and also so that supervisory staff can acquire appropriate knowledge and experience to oversee and validate the work of other election staff effectively.

Asset Management

It was noted in the course of the Commission’s review that there is some uncertainty as to the formal ownership of the equipment held locally by each returning officer. As a specific budget was allocated to each returning officer to meet the purchase cost of the equipment delivered directly to them by the Manufacturers, some returning officers believed that ownership was officially theirs while others believed that the equipment belonged to the State, to the Department or to the Department of Finance which provides funds generally to returning officers.

In asset management and security management terms, ownership is an essential and fundamental principle that needs to be clearly established so that the rights, obligations and responsibilities that follow from it can be clearly assigned. This is particularly relevant in the context of implementing security controls and a comprehensive overall security policy in respect of the distributed assets of the chosen system.

Consistent with ownership is the concept of maintaining clear records of the identity, location and movement of assets. In the case of a distributed system such as the chosen system that is coordinated for use at national elections under centralised policy guidance, it would be important that such a record is capable of being administered both locally and centrally.

The Commission’s auditors observed that, although most returning officers have records of the equipment that was assigned to them and some of these are very detailed and accurate, there is uncertainty in some cases as to how many equipment items were actually delivered, their identification by serial number and how many remain following various incorrect deliveries, returns for maintenance and other movements, etc., of equipment that may have occurred. The auditors also obtained access to global records held by the Manufacturers and the Department regarding the numbers of voting machines assigned to each location, but it was observed that in a number of cases the number recorded in respect of a particular site differed from the number actually present. In a spot check query of the Manufacturers' records seeking details of particular equipment items, a manual search of the paper records was unsuccessful in locating the information sought.

A single central asset register recording the identity, ownership, storage location, movement, deployment at elections, maintenance history and other details of each item of electronic voting equipment would allow precise numbers to be determined and would also allow periodic audits to enable full inventory control.

Consistent with the establishment of an asset register is the implementation of more rigorous control procedures for the movement of equipment and votes at election times, as already noted above. Each voting machine, ballot module and CD should be accompanied by a control sheet at all stages of an election on which should be recorded and authenticated the identity of the persons who are responsible for the transport and control of the device and other relevant details regarding its use at each stage. These records should subsequently become part of the central asset register.

Risk assessment is also an important security policy management issue. By identifying particular threats to the equipment and its storage locations, risk assessment can inform the implementation of appropriate security measures. Threats to the chosen system need to be considered both locally and at national level. However the Commission's auditors observed that no person or body currently involved in the storage and deployment of the chosen system has the capability to gather intelligence on threats that may be present in various different locations and in national and local contexts. An assumption is made in most cases that there is currently no impending threat but these assumptions are not made on the basis of information from informed sources. This could be addressed at national level by liaison between the Department and relevant government or third-party security agencies, and addressed locally by liaison between returning officers and local Garda crime prevention officers.

The Commission's auditors observed that, at the time of the audit, rent, utility bills and monitored alarm services had in some case remained unpaid for some months and there was some uncertainty surrounding whether these and insurance policies that would soon fall due for renewal should be paid. It is likely that, if these and related costs remain unpaid for any extended period, the provision of power, heating, alarm and monitoring services would cease, resulting in significantly higher risks that voting equipment may be damaged, interfered with or stolen.

There was also significant divergence across constituencies on the perceived need for insurance cover in respect of equipment. While some returning officers had taken out specific cover in respect of fire, damage or theft, others had taken no cover. Some of those who had taken no cover were of the view that all equipment was covered by the State or by the Department.

4.3 Findings on Physical and Operational Security

This section summarises the Commission's findings in relation to physical and operational security aspects of the chosen system based on the work described in *section 4.2*.

Manufacture and Transport

Hardware and Embedded Software

Nedap has sought to adopt best practice in terms of preventing unauthorised access to its premises. Secure areas have been designated and sufficient controls appear to be in place to prevent unauthorised third parties from gaining access to the development, manufacturing and assembly facilities at which the hardware and embedded software components of the chosen system are produced.

There is a critical reliance of Nedap's hardware and embedded software components on the availability and reliability of the election management software supplied by Powervote Ireland Ltd.

Election Management Software

Development and maintenance of the election management software is undertaken in a home office environment where the physical and logical access controls are usually below those that would be found in a secure commercial development environment.

The apparent lack of formal software development or change control procedures also places heavy reliance on the knowledge and memory of the product as vested in the developer.

Transport

There is a potential risk to the security of voting equipment (hardware and embedded software) that is unaccompanied and/or unattended while in transit from the Manufacturers by road and sea internationally and also during local delivery to individual returning officers.

The manual records kept by the Manufacturers in respect of the transportation of such voting equipment are not easily referenced against the location of specific machines in Ireland. These records would benefit from being transferred to a computer system already implemented by the Manufacturers in respect of voting equipment supplied to the Dutch government.

The transfer of the election management software from the Manufacturers to the Department and/or its agents by e-mail is not an appropriate method by which to convey such sensitive material.

Storage

Accommodation

The availability of suitable long-term storage for electronic voting equipment in most constituencies is limited. Returning officers are rarely in direct control of the environmental or immediate surroundings and few have direct control of the buildings in which storage is provided. This limits the controls that can be implemented at the outer physical security layers and places a greater emphasis on the importance of measures implemented at, and within, storage premises to deter, prevent, detect, delay and respond to unauthorised access or attempted access to voting equipment.

Expertise and Training

Specific training and guidance on appropriate security measures in the context of electronic voting equipment containing sensitive data has not been provided to returning officers although many returning officers have a clear understanding of what is required, regardless of whether or not they are able to provide it.

There is, as a result, some inconsistency of the security measures implemented within individual storage locations and, generally, across different locations.

Security Measures Implemented

The most important measure that needs to be considered in light of this variance in security levels is that of detection. If unauthorised access is detected, then appropriate measures can be taken to deal with any threat that may result. If such access remains undetected, there can be potentially serious results for the conduct of elections and the credibility of the electronic voting process. The implementation of two layers of physical detection with appropriate maintenance and testing or, alternatively, manned supervision would meet this requirement.

Not all storage facilities include provision for monitoring and control of temperature and humidity conditions in accordance with the specific guidance provided by the Manufacturers. Although extremes of tolerance have been specified in respect of the equipment, it has also been indicated that long-term exposure to these extremes, or rapid changes of ambient conditions are not advisable.

The arrangements whereby voting equipment is currently stored at 25 locations are likely to give rise to continuing variations in the implementation of security and related control measures, together with replication of similar costs of implementation of these measures which are not insignificant across individual centres. Enhanced and more uniform security and greater economy of security costs could be achieved through the rationalisation of storage on a regionalised or centralised basis.

Voting machines are at greatest risk when they are stored following their configuration with programmed ballot modules for use at an election. Complete assurance of the security of the equipment is thus required between the time they are programmed and the time they are used, including during transportation to polling centres.

Use at Elections

Set-up and Programming

There is a lack of rigour and clarity in the procedures governing the version control, installation and exclusive use of the election management software on the hardened PC and in the procedures surrounding the use, maintenance and re-use of the hardened PC exclusively for election purposes.

The controls on the proposed use of CDs to transfer sensitive election data between returning officers in the course of preparations for the poll require to be brought up to a higher standard. These controls should be in keeping with those recommended further below in respect of transporting ballot modules and CDs containing votes, but with appropriate modifications having regard to the fact that the transport of votes is not involved at this stage.

Transport and Use in Polling Centres

The arrangements for the transport of programmed voting machines to polling centres need to take account of the differences in security requirements that exist under electronic voting as compared with paper voting. Programmed voting machines are more vulnerable to interference or accidental damage than the former ballot boxes, they are also considerably larger to accommodate and there are additional health and safety considerations associated with their handling and set-up.

Although the risks to security of the voting equipment while it is in use at polling centres are low and the likelihood of deliberate damage or sabotage is also low, a number of health and safety issues for election staff and voters have been noted in the context of such use.

The importance of maintaining security around the voting machine after the ballot module has been removed and at least until the votes have been successfully read in needs to be emphasised, as the voting machine contains the backup ballot module which is required in case of failure or loss of the primary ballot module. It may also be necessary in any subsequent review to verify that the voting machine has not been tampered with and that it remains as it was while in use by voters.

Transport of Votes on Ballot Module and CD

Transport of the ballot module from the polling centre to the read-in and count centre is the most sensitive stage in the entire life-cycle process of the chosen system. There is a low risk associated with the main theoretical threat of the substitution of a ballot module that has been programmed with bogus votes by a person with access to the election management software and a programming/reading unit. However there are also the threats of accidental or deliberate damage, destruction or loss of the ballot module which, notwithstanding the existence of a backup ballot module, can have an impact on confidence in the electronic voting system.

The physical security measures for the transport of ballot modules thus need to be strengthened by the implementation of controls including tamper-proof or tamper evident packaging with uniquely identifiable seals and authenticating documentation, the provision of Garda or equivalent security escort and procedures for authenticating the identities of not less than two specifically nominated election staff to carry out collections.

While the risk of unrecoverable loss of votes is considerably diminished in the case of the numerous CDs containing votes which are transmitted from read-in centres to count centres, there are fewer obstacles in terms of the technology required by a person seeking to intercept and either substitute or alter the votes contained on a CD. Conversely, there are more votes contained on a CD than on a ballot module and the potential impact on confidence in the system would be proportionately greater in the event of any such attack. The logical and physical security measures implemented in respect of CDs thus require to be at least as strong as those implemented in respect of ballot modules.

Read-in, Counting and Disposal of Votes

The security arrangements at read-in and count centres, together with the procedures for the inputting of postal votes, need be generally prescribed to minimise any risk of accidental or deliberate substitution, alteration, loss or destruction of votes. Although such undesirable events will in most cases be recoverable once detected by administrative procedures, the visibility of official proceedings at read-in and count centres is high while the transparency in terms of people's ability to observe the actual electronic handling of votes is low. There is therefore an enhanced requirement to take every necessary physical and operational security measure to ensure confidence in the integrity of the processes.

Careful attention is required to the custody and recorded disposal of sensitive data following an election, including as regards the distinction that multiple copies of each vote exist under the electronic system and the statutory requirement that votes be retained for six months and then destroyed. These requirements are consistent with the requirement further below for the preparation and maintenance of an asset management register in respect of electronic voting equipment.

Security Policy Management

In addition to assessing the direct physical and operational security measures implemented in respect of the chosen system, the Commission's auditors also made general observations on security policy management, highlighting that attention is required in the following areas:

- provision of guidance and training to returning officers, including security training;
- pooling and coordination of knowledge and experience between returning officers;
- selection and security vetting of election staff and third party service providers;
- re-training in use of equipment;
- clarification of ownership of equipment and consequent entitlements and responsibilities;
- establishment and maintenance of a central asset register of all electronic voting equipment;
- implementation of documentary control procedures on equipment movements at elections;
- assessment of risks to equipment at local and national levels;
- clarification of requirement to insure equipment.

4.4 Conclusion on Physical and Operational Security

This section sets out the Commission's conclusion on physical and operational security aspects of the chosen system. The Commission's conclusions arising from its work in relation to other aspects of the chosen system are set out, in each case, at the end of the other relevant parts of this report. The Commission's overall conclusion on the chosen system is set out in *Part 7*.

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.

On the basis of the assessment of the physical and operational security of the chosen system by auditors appointed by the Commission, the following areas for further improvement have been noted:

- 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.

This conclusion on physical and operational security of the chosen system has been drawn, and should be interpreted by others, in the context of the Commission's conclusions arising from other aspects of its work set out elsewhere in this report. This includes the Commission's work on technical aspects and testing (*Part 3*) and the comparative assessment of the chosen system and the paper system (*Part 5*). These conclusions are also incorporated within the Commission's overall conclusion on the chosen system in *Part 7*.