CHAPTER TWO:

Introduction to Electronic Technologies in Elections

INTRODUCTION

Every electronic device used in elections operates and interacts with a variety of inputs in a set of circumstances that provides a context or "*environment*." In order to understand the interaction between election officials, voters, political contestants and electoral technology, observers must examine and analyze the environment in which the equipment is being used.

As noted above, any technology is one part of a broader electoral environment, where human interactions largely determine environmental quality. Knowledge of the electoral choices, the presence or absence of intimidation, the competence and integrity of electoral officials at all levels are among the environmental factors that have direct and substantive impact on the performance of electronic technologies in elections. Monitoring electronic technologies therefore cannot be isolated from the broader electoral and political context. However, just as proper application and performance of electronic technologies can take place in an otherwise fraudulent election, an otherwise proper election can be derailed by fraudulently manipulated or faulty electronic technologies.

A technological environment can be classified as either *controlled* or *uncontrolled*. For an electoral environment to be considered controlled, it is generally accepted that it must meet all of the following criteria:

- Representatives of political contestants, nonpartisan domestic election monitoring organizations and other appropriately authorized persons are physically present, and are able to access and observe the environment.

- Election officials are present, in charge of the process and have legal responsibilities and powers to ensure the accuracy and integrity of the electoral process.

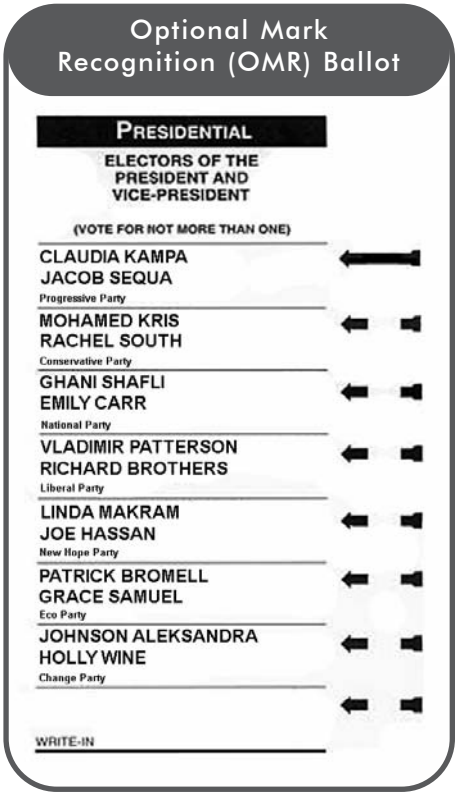
- Access (whether physical or virtual) to the environment, including the technological devices, is secured and controlled, and is regulated by a process that is independently auditable and verifiable.

An example of a *controlled* environment is a polling station where secured electronic voting devices are used, and the polling station staff are liable for the proper functioning of the devices. Party and/or candidate agents, as well as nonpartisan election observers, are present, understand and monitor whether the electoral procedures are properly followed. The electronic devices must not be in a network, and they must be restricted so that they do not interact with other computers (and are thus "isolated"). Interaction restrictions must be safeguarded with the use of hardware and software with security features, and the administration of devices must fall under established security protocols.

Environments can be classified as *uncontrolled* if any of the following exist: representatives of political contestants, nonpartisan domestic election monitoring organizations and other appropriately authorized persons are not physically present, and are not able to access and observe the environment; election officials are not present, not in charge of the process or do not have legal responsibilities and powers to ensure the accuracy and integrity of the electoral process; and access (whether physical or virtual) to the environment, including the technological devices, is not secured and controlled, and is not regulated by a process that is independently auditable and verifiable. Examples of uncontrolled environments are on-line voter registration or voting through the Internet. In both cases, the environment is uncontrolled because election officials are not present to authenticate the identity of the voter and supervise use of devices, and the data transmission is occurring over an open network.

OPTICAL MARK AND OPTICAL CHARACTER RECOGNITION

The basic principle behind Optical Mark Recognition (OMR) and Optical Character Recognition (OCR) technology is for the equipment to turn marked data or hand written data into electronic records. OMR and OCR devices are commonly used for processing voter registration forms and counting votes.



OMR devices are machines that capture data by scanning and recognizing a set of predetermined marks on a sheet of paper. In the electoral context, voters are asked to indicate their choice by placing a specific mark on the ballot paper. The ballot papers are then fed through the OMR device, and the machine is able to quickly recognize the marks and tabulate the results. For example, voters are asked to connect the arrow in front of the candidate of their choice by filling in a space.

OCR devices function similarly to OMR machines, but they record data by scanning and recognizing written letters rather than predetermined marks. This technology is sometimes employed in voter registration processes. It can also be used to read "write in" names on ballot papers.

OMR devices are generally considered to yield more accurate results than OCR devices because they are designed to identify specific marks in a set of predetermined places, whereas OCR devices must recognize hand writing, which differs from individual to individual. This requires the device to interpret the written responses of voters and can lead to higher error rates. On the other hand, the OCR system is designed to read more complex information and thus can be used by election administration officials for a multiplicity of purposes, including recording names and other information on voter registration forms.

When OCR devices are used in voter registration, the record should then be verified for error correction by comparing the information

with the written record. This is often accomplished during the claims and objections period, when citizens can review entries on a preliminary voter registry and request that errors be corrected. If OCR technology is used to read write-in names on ballot papers, the verification should be done immediately by election officials in the presence of political party/candidate agents and nonpartisan election observers to meet the requirements for a controlled environment and ensure electoral integrity.

Scanned ballots from OMR devices should be reviewed by election officials in the presence of party/candidate agents and nonpartisan observers to ensure votes recorded on rejected ballots or votes not recorded though marked are properly included into the overall count, and the counting results recorded on the devices should be verified by a reliable method to ensure that they correspond to the ballots cast. For example, a statistical sample of devices could be selected and verified against the ballot, while all rejected or non-counted ballot choices could be reviewed on the spot. Such methods are discussed below in Chapter 4.

PUNCH CARD SYSTEM

A punch card system requires that voters punch a hole in the ballot paper to indicate their choice. The ballot is then fed into a counting device, similar to an OMR device, that reads which hole has been marked and translates that information into an electronic record. This data is stored in the memory of the device.

An issue that emerges with this technology is whether the ballot is properly designed so that the voter actually punched the hole that corresponds to the candidate or party of his or her choice. Another critical issue that emerges with this technology is whether the platform on which the punch card ballot is placed allows the voter to punch the hole completely through the card, thus ensuring that the voter's choice is accurately read by the counting device.

The punch card ballots should be inspected in the view of political party/candidate agents and impartial observers to determine whether a ballot choice was improperly omitted by the device because the card was not sufficiently punched. This may be decisive in close elections. In addition, the software used for counting should be

subjected to verification by reliable means and compared to the choices indicated on the punch cards, just as paper ballots should be compared to scanned results recorded on OMR devices. A post-election statistical sample of machines and punch cards should be reviewed to determine error rates, thus examining the effectiveness of the technology, even if there are no electoral challenges.

DIRECT RECORDING ELECTRONIC (DRE) SYSTEM

Direct Recording Electronic (DRE) systems are a type of technology that requires the voter to use a keyboard, touch-screen machine, mouse, pen or other electronic device to indicate their choice. Using such systems, a voter produces an electronic record of their vote rather than marking a paper ballot. The DRE device can be built to produce a paper record of each vote, including a paper record that can be reviewed by the voter before registering her or his vote. The paper record is then stored in the machine for verification purposes. An emerging consensus is developing to employ this approach when using DRE technology because it allows for recounts and other vote verification techniques that meet transparency requirements and enhance public confidence. As with OMR and punch card technologies, DRE machines should be subjected to post-voting verifications.[8]

Direct Recording Electronic (DRE) system
Source: Agencia Brasil/José Cruz

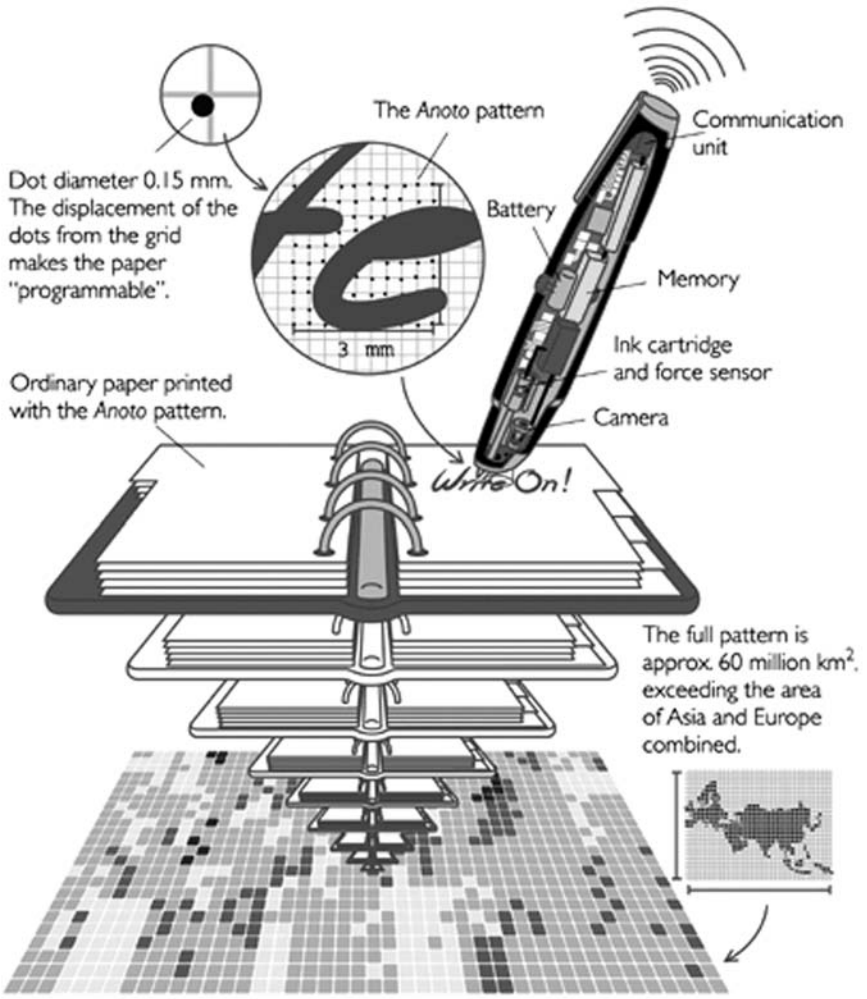
DIGITAL PEN

The digital pen is a DRE device that creates an electronic record while simultaneously marking specialized paper. The device recognizes and records the movement of the pen's point and at the same time leaves an ink trail on the paper. The paper contains microscopic dot patterns that allow the digital pen to recognize the position of the mark on the digital paper. Data stored in the pen can then be uploaded to a computer and software transforms the data into text.

[8] Please see Chapter 4 for further discussion of these subjects.

Digital Pen

Source: Anoto Functionality © Anoto Group AB



PAPER RECORD

A paper record (sometimes called Paper Trail, Audit Trail or Voter Verifiable Paper Audit Trail — VVPAT) is a printed record of a voter's action of touching the keyboard or screen - whether this record concerns the person's vote or his or her voter registration record. It is important to note that unlike OMR and OCR devices, a paper record is produced after the voter has entered her or his information into the DRE device. With DRE technology, the creation of the electronic record precedes the paper record.

There are different interpretations about the relationship between the electronic record of a vote and the paper record, when using DRE

technology. The legal status of the paper record is of fundamental importance to determining the overall integrity of the electoral process.

Equipping a DRE voting device with a paper audit trail capability is widely viewed as a basic requirement for ensuring transparency in the voting process. This, however, is not an infallible safeguard for electoral integrity, and precautions are required to ensure that the paper record is not manipulated. Nonetheless, if there is no reliable verification method, election results could be inaccurate - based on innocent error or fraud - and there would be no effective means to settle contested issues.[9]

If the DRE voting device does not produce a paper record, this is usually called "Black Box Voting."[10] It is generally agreed that such voting techniques do not provide a sufficient means for voters and political contestants to know whether the technology accurately represented the will of those who voted. In addition, should there be a reason to contest the outcome of an election where Black Box Voting is used, there is no reliable means to determine whether the voter's will was respected. This means that organizing new elections would likely be the only effective remedy, which is highly burdensome, expensive and unlikely to recreate the result that voters chose on the designated election day.

ENTRY AND TRANSFER OF DATA

At any stage in the electoral process where data is collected and stored electronically at the polling station level, data will need to be transmitted to higher levels either by electronic or physical means. Electronic methods to transmit data recorded during an election or voter registration process include telephone lines, radio waves or computer networks. Physical transmission involves the transportation of actual data in storage modules (e.g., memory cards, optical media or magnetic media) to the tabulation centers.

---

[9] Please see Chapter 4 for further discussion of these issues, including monitoring techniques.

[10] In Belgium, voters are given a data memory card at polling stations where e-voting is conducted. The voter places the card in a machine inside the polling booth. The machine registers the voter's choices on the data card - not on the machine. Voters then take their data cards to an electronic ballot box, which reads and records the votes on its memory device and a CD. The electronic ballot box keeps the voters' data cards, which could be used in a recount. No voter verifiable paper audit trail (VVPAT) is used in this system, although this is not "Black Box Voting." A number of issues are presented by the system, including among others the accuracy of data recorded onto the card, the accuracy of how the card's data are read and registered by the electronic ballot box device and the method of vote tabulation. Please see the Country Note in Chapter 4 of this Guide for further description of Belgium's system.

The type of transfer is important because it will determine whether the environment is controlled or uncontrolled, which has an affect on the overall integrity of the electoral exercise. For example, transferring data over public networks, such as the Internet, is performed in an uncontrolled environment, because the devices are networked with numerous computers and servers. Even semi-closed networks, such as governmental networks, are essentially uncontrolled.

If sealed memory cards (or other electronic media or whole devices) are transported by election officials in a secure manner in the presence of party agents and nonpartisan observers, the data would be transferred in a controlled environment. If the environment is uncontrolled at any stage in the transfer, records will be exposed to the potential of entering different input, and therefore to different threats of corruption.

As with the Voter Verified Paper Trail, it is a good practice to back up an electronic record with the paper record. If the counting of votes is performed at the polling station, it would be advisable that the paper record is compiled and transferred along with the electronic one.

Monitoring of data entry and transfer is critically important. As with ballot boxes, memory cards, optical media or magnetic media used to record sensitive information, such as votes or voter registration information, should have unique identifiers and other safeguards to ensure that they are not switched during the electoral process and should have special security mechanisms to ensure against the corruption of data. Before sensitive data is entered, such as recording votes, the cards or other electronic recording media should be inspected to ensure that they are "empty" (politically neutral) before voting begins. These electronic recording devices should be inspected in the presence of party/candidate agents and impartial observers to establish that they do not contain pre-recorded votes or instructions that would corrupt the election. Tests for corruptions should be conducted by reliable methods before and/or on Election Day in the presence of party/candidate agents and impartial observers.

Using uncontrolled methods like the Internet or semi-closed governmental networks to transfer sensitive electoral data multiplies

possibilities for interception and corruption of data. Such means of data transfer require robust encryption systems. If memory cards are removed from electronic devices, the cards can be switched with pre-programmed cards or can be modified before the data is transferred - just as ballot boxes can be switched or stuffed in transport. Special safeguards need to be employed to secure and seal memory cards (just as ballot boxes are sealed and their identity numbers are recorded). This should be done under the view of party/candidate agents and impartial observers. The transport of sealed memory cards with unique identifiers should be accompanied by such monitors. It is generally accepted that the transfer of voting data should occur only after the polls have closed and not during the voting process. Internet voting is an exception to this practice (see below).

THE INTERNET IN ELECTION PROCESSES

Voter Registration:

The Internet as a global public network is increasingly important in the electoral process. Election officials are using the Internet to register voters,[11] display voter lists or individual voter registration records[12] and communicate polling station assignments to voters.[13] Entering voters' relevant information on the spot at registration centers into Direct Data Capture (DDC) devices that allow transport of the data to create a centralized voter registry can facilitate the registration process, and that data transfer is sometimes done via the Internet.[14]

Using the Internet to display voter lists or individual voter registration records can provide an effective means for political competitors and citizens to check the voter lists and verify their accuracy. This can provide the basis for requests for corrections to errors in individual data, to add data concerning individuals who were improperly omitted from the registry and to challenge the appearance on the voter registry of people who died, or the existence of multiple entries for one person or the appearance of persons who are ineligible. As

[11] E.g., State of Arizona (US), Province of British Columbia (CA), Hong Kong SAR.
[12] E.g., Croatia, Palestinian Territories.
[13] E.g., South Africa.
[14] Security issues discussed above concerning transporting such data over open networks or transporting sealed memory cards (or other recording media) apply to voter registration data as well. It is therefore important that the process be transparent to party/candidate agents and impartial observers as the data is recorded and that they are able to verify the security of data transfer. Please see Chapter 3 for further discussion of these issues.

will be discussed later in this Guide, electronic copies of the voter registry can also be provided in a number of forms to political contestants and to impartial election monitoring organizations, so that they can conduct verifications of the registry and assist citizens to check the voter lists and request corrections. These activities contribute to heightened public confidence in the voter registry.

Internet Voting:

Internet based voting presents significant security concerns, where "hacking" and other means of corrupting data appear thus far to overcome the benefits of using this technology in elections for public offices. In addition, serious problems concerning secrecy of the ballot arise in Internet based voting. Therefore, in the view of most experts at this time, Internet based voting is not an acceptable electoral technology.[15]

In very limited examples, the Internet has been used for voting, though Estonia is the only example to date where the Internet has been used for general voting in elections for public office.[16] As mentioned above, Internet based electoral technologies operate in uncontrolled environments. For example, "Remote Internet Voting" is where a voter can vote from any computer that has access to the Internet. In these circumstances, there is no oversight by election officials, which means that voting takes place in an uncontrolled environment. This has serious implications for maintaining the secrecy of the ballot.

"Poll-site Internet Voting" is a system where a voter votes via the Internet, but only in a polling station designated to the voter, with computers provided by and under legal control of election officials. "Kiosk Voting" is basically the same as Poll-site Internet Voting, except voters can choose to vote at any polling place in the election district. These are attempts to create partially controlled environments, but many of the risks to electoral integrity remain unaddressed.[17]

---

[15] For an excellent overview of threats and weaknesses of Internet voting, see David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner, *A Security Analysis of the Secure Electronic Registration and Voting Experiment*, Carnegie Mellon Institute for Commerce (January 5, 2004), available at http://euro.ecom.cmu.edu/program/courses/tcr17-803/MinorityPaper.pdf.

[16] It has been allowed for those citizens who possess national ID card with an integrated chip. Internet voting is available in Switzerland, UK and Canada, but it is limited to certain voters or local elections. Please see http://db.e-voting.cc for further information.

[17] Please see Chapter 4 for further discussion of Internet voting and related monitoring issues.

Displaying Voting Results:

Election officials sometimes use the Internet to post election results. Partial unofficial results, as well as complete official results, are increasingly posted on the websites of election authorities. When this is done, it is particularly important to post the disaggregated results (i.e., polling station-by-polling station results for each electoral contestant), as well as the aggregated results. This allows analysis by the political contestants, impartial election monitors and the news media to understand where the results reported came from and to understand what areas have not yet been recorded. This can help prevent premature expectations of victory and premature disappointments and corresponding reactions that can destabilize an electoral environment. In addition, posting disaggregated results allows political contestants and impartial observers to compare polling station records with the copies of results they collected through their agents (poll watchers and observers). This builds confidence in the accuracy of the vote tabulation and results reporting by election officials.

SPECIFIC STANDARDS FOR ELECTRONIC VOTING

Given that internationally recognized standards for electronic voting do not yet exist, countries utilizing such technology are developing their own principles and guidelines. Important elements for discussing standards for equipment, technology and procedures on a national level include the following:

- LEGAL FRAMEWORK requirements that are prescribed by the election laws and other national laws and electoral administration bylaws and regulations;

- TECHNICAL REQUIREMENTS and specifications developed by electoral administration;

- PRINCIPLES FOR DEMOCRATIC ELECTIONS set forth in international instruments and developed by international organizations;

- PRODUCTION STANDARDS of manufacturers;

- INFORMATION TECHNOLOGY STANDARDS developed by expert and standards setting organizations.

To date, the most significant multinational attempt to develop international standards for electronic voting is the "Recommendation of the Council of Europe Rec (2004) 11."[18] This document and the corresponding associated Explanatory Memorandum provide non-binding recommendations to the member states on how to implement electronic voting. Rec (2004) 11 deals with a very broad set of issues and includes legal, operational and technical standards.

It is noteworthy that the Council of Europe (CoE) Recommendation endorses the use of EML 4.0, Elections Markup Language[19] developed through an open process by the Organization for the Advancement of Structured Information Standards (OASIS[20]). EML is a standard for the structured interchange of data among hardware, software, and service providers who engage in any aspect of providing election or voter services to public or private organizations. The services performed for such elections include but are not limited to voter list maintenance, redistricting, requests for absentee/expatriate ballots, election calendaring, logistics management, election notification, ballot delivery and tabulation, election results reporting and demographics.

In the United States, there is a shared responsibility between the three levels of government in overseeing the conduct of elections. Each state sets its own guidelines for the conduct of local, state and federal elections. In turn, states have generally delegated the authority to conduct elections to smaller subdivisions, such as counties, cities or towns. As a result, there are thousands of jurisdictions that administer federal elections throughout the country. However, states must comply with requirements set forth in certain federal legislation in order to receive funding for electoral matters and concerning certain elements of federal elections. The Help

[18] Recommendation Rec (2004) 11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and Explanatory memorandum on Legal, Operational and Technical Standards for E-Voting. Please see Appendix 3 of this Guide for an excerpt of REC (2004) 11.

[19] See Cover Pages, *Election Markup Language*, (last modified August 14, 2007), available at http://xml.coverpages.org/eml, for an overview of the design goals and standards of EML 4.0, the Election Markup Language developed by OASIS and approved by the Election and Voter Services Technical Committee.

[20] OASIS (Organization for the Advancement of Structured Information Standards) is a nonprofit, international consortium whose goal is to promote the adoption of independent standards for information formats (www.oasis-open.org). For more information, please see Appendix 2 of this Guide.

America Vote Act (HAVA), for example, mandates federal standards[21] for the functionality, accessibility and security of voting systems across the country, as well as for allocating funds to states to help upgrade outdated equipment.[22] HAVA is not exclusively an electronic voting standard; it addresses other types of voting. HAVA established the US Election Assistance Commission (EAC), which-in cooperation with the National Institute of Standards and Technology (NIST)—is developing voluntary guidelines for voting systems. The voluntary voting system guidelines (VVSG) will provide a set of specifications and requirements that voting systems, voting devices and software must meet to receive a certification from the EAC. Under HAVA, adoption of the VVSG by the U.S. states would be voluntary. Nonetheless, states may adopt the VVSG and make them mandatory within their jurisdictions. EAC accredited laboratories will test electronic technologies against the VVSG and provide a recommendation to the EAC, while the EAC's Executive Director will make the decision concerning whether to issue a certification. When activated, this will be the first time that federal authorities will test and certify voting systems. Previously, voting systems were tested and certified by companies qualified by the National Association of State Elections Directors (NASED).[23]

INFORMATION TECHNOLOGY STANDARDS

There are many recognized private, public, national and international institutions that are developing standards for information technology (IT). The largest and most developed is International Organization for Standards (ISO), but there are many more recognized by the IT industry.[24] These standards, however, are not specific for electronic elections systems or specific products. They deal, for example, with process, security requirements, management certification and audit processes.

---

[21] Although HAVA is legally limited to federal elections, in practice it influences virtually all elections in the US. It addresses requirements for the electronic voting such as: testing, certification, decertification, and recertification of voting system hardware and software. Also, voting system standards and requirements are addressed (in Sec 301). See generally, Help America Vote Act (HAVA), 42 U.S.C. § 15301 (2002).

[22] There are numerous relevant bills currently in the U.S. federal legislative process (e.g., Voter Confidence and Increased Accessibility Act of 2005, Voting Integrity and Verification Act of 2005 (VIVA 2005), Count Every Vote Act of 2005, Voting Opportunity and Technology Enhancement Rights Act of 2005 (VOTER Act of 2005), Know Your Vote Counts Act of 2005, Verifying the Outcome of Tomorrow's Elections) and many before the State legislatures.

[23] "EAC Seeks Public Comment on TGDC's Recommended Voluntary Voting System Guidelines," U.S. Election Assistance Commission Press Release (31 October 2007) (www.eac.gov).

[24] For example, Institute of Electrical and Electronics Engineers (IEEE), NIST, European Committee for Standards (CEN), and OASIS. See Appendix 2 of this Guide for more information.

IT specialists who are engaged in evaluation of the electronic voting and other IT systems in electoral process should be acquainted with these standards, as they provide internationally recognized framework. Election monitoring specialists associated with political contestants and impartial observation organizations should be familiar with these standards to better evaluate some components of the electronic elections system, though they do not provide information concerning how specific elections equipment or software should be built or should perform.