ODIHR.GAL/73/08
28 October 2008

ENGLISH only

Office for Democratic Institutions and Human Rights

OSCE/ODIHR DISCUSSION PAPER IN PREPARATION OF GUIDELINES FOR THE OBSERVATION OF ELECTRONIC VOTING

Warsaw
24 October 2008

TABLE OF CONTENTS

OSCE/ODIHR DISCUSSION PAPER IN PREPARATION OF GUIDELINES FOR THE OBSERVATION OF ELECTRONIC VOTING

24 October 2008

I. INTRODUCTION

The OSCE/ODIHR has developed a comprehensive methodology for observing elections in OSCE participating States.[1] The OSCE/ODIHR election observation methodology is consistent and considers all phases of the election process before, during and after election day. The methodology also provides various options for effectively assessing an election process in accordance with the requirements of each election. An Election Observation Mission (EOM), with a full complement of election experts, long-term observers and short-term observers, is deployed if it is necessary to make an assessment of an election process in its entirety.[2] An Election Assessment Mission (EAM), composed of a team of election experts, is deployed when it is necessary to focus on specific issues within an election process.[3] As a result of its methodology, the OSCE/ODIHR has been able to formulate sound conclusions concerning election processes and accordingly make meaningful recommendations for possible improvement in the respective OSCE participating States' elections.

The emergence of electronic voting systems[4] can present opportunities to election administration to enhance voter participation and access, and can be particularly pertinent in instances with multiple elections conducted simultaneously. However, such potential advantages are only beneficial to an electoral process if such technologies can be introduced in a manner compatible with the principles enshrined in the OSCE

---

1 OSCE/ODIHR Election Observation Handbook, Fifth Edition, Warsaw, 2005.

2 In an OSCE/ODIHR EOM, the core team of experts, together with long term and short term observers, assesses all phases of the election process, including the political context; legislative framework; performance of the election administration; voter and candidate registration; election campaign; media; voting, counting, and tabulation; and the consideration of complaints and appeals. The core team of experts is usually deployed six to eight weeks before election day. Long term observers (LTOs) are deployed a week later and provide balanced geographical coverage of the country. They observe the pre-election environment and campaign activities leading up to election day. A larger contingent of short term observers (STOs) is deployed shortly before election day, after a comprehensive briefing on the ground, to observe polling, counting, and tabulation of results in polling stations and election commissions. LTOs and STOs are deployed in international teams of two. Based on collective findings, an EOM is able to consider whether any reported irregularities or violations of law are isolated incidents or whether they form a systematic pattern that could pose a threat to the integrity of the election process. As a result, the EOM can assess the extent to which the electoral process was carried out in a manner that enjoyed the confidence of the candidates and the electorate, as well the degree of political will demonstrated by the authorities to conduct a genuine democratic election process in accordance with OSCE commitments.

3 In an OSCE/ODIHR EAM, a team of election specialists deploys from one to four weeks prior to election day. The EAM looks at the election process as a whole, but focuses on issues that may be of particular significance in that country, such as the conduct of the campaign in the media, the participation of national minority groups, campaign finance, voter eligibility or other issues.

4 For the purposes of this paper, the term "electronic voting" is intended to be broad and include new technologies for casting, counting, and tabulating ballots. *See* Part II of this paper for a more detailed description of "electronic voting".

commitments and other international standards for democratic elections, and offering the same guarantees for transparency, accountability and public confidence as traditional voting methods. In this context, new voting technologies can pose challenges not only to election administration but also to election observation.

Transparency is a cornerstone of the election related commitments agreed by all OSCE participating States in the 1990 Copenhagen Document, and observation is a key aspect of transparency. Transparency is necessary to "ensure that votes are cast by secret ballot or by equivalent free voting procedure, and that they are counted and reported honestly with the official results made public".[5] Further, the OSCE 2003 Maastricht Ministerial Council has noted the need for accountability and confidence by the electorate in the entire election process.[6]

Electronic voting poses challenges to the traditional and broadly accepted concepts of transparency and accountability of election processes. It has also become the subject of public debate in a number of countries, thereby influencing public perceptions and confidence concerning the security and secrecy of the ballot and the reliability of electronic voting.

The obvious challenge of electronic voting, in terms of transparency and accountability, is that it is more difficult to observe. Electronic events take place that are not subject to ordinary examination with the naked eye of an observer. Further, electronic voting consists of technological components that are not readily nor easily understood by the average observer. In contrast to the simplest voting system, which consists of people, pens, and paper, an electronic voting system includes elements which are not directly observable.

Furthermore, the OSCE/ODIHR election observation methodology has always taken into consideration the element of public confidence in elections and election administration when assessing an election process. This element of elections acquires a heightened level of consideration where ballots are cast, counted, or tabulated electronically.

It is thus critical for election observation to keep pace with the emergence of new technologies, as a democratic election requires the exercise of universal, direct, equal, and secret suffrage through the casting, counting, and tabulation of ballots in a transparent and accountable manner. The consideration and introduction of new voting technologies in an increasing number of OSCE participating States, as well as the real challenges such technologies can pose for ensuring respect for fundamental election-related commitments, justifies the development of specific guidelines for observation of new voting technologies. The value of harnessing new technologies to enhance electoral processes very much depends on the existence of safeguards commensurate with those offered by traditional voting methods, in order to achieve full respect for OSCE commitments.

The development of guidelines for observation of electronic voting systems is important in order for an OSCE/ODIHR election observation or assessment mission to properly assess such specific elements in an election process, as relevant to the overall assessment.

---

5 See Paragraph 7.4 of the 1990 Copenhagen Document.

6 Decision No. 5/03 (2 December 2003).

However, while new voting technologies may underpin fundamental aspects of an election process, guidelines should not be developed to the disadvantage of other fundamental aspects of the process that should always be an ongoing focus of an election observation mission's attention. In addition, guidelines should not be interpreted as OSCE/ODIHR's endorsement of electronic voting systems as such.

Consistent with its current election observation methodology, a balanced approach that incorporates meaningful and effective access for observers, but also non-interference of observers in the process, should also be the basis for the OSCE/ODIHR's observation of electronic voting systems. Also, guidelines for observing electronic voting must reflect the fact that election observers do not certify electronic voting systems and / or election results.

This discussion paper is part of an ongoing process to further develop OSCE/ODIHR observation methodology for observing new voting technologies.[7] It identifies areas that should be considered in order to enhance the OSCE/ODIHR observation methodology where electronic voting is an element of a participating State's election process. Minimum requirements for transparency, accountability and public confidence, in the context of new voting technologies, are discussed as well.

---

[7] Relevant OSCE documents in this respect include

1) the 2003 ODIHR report *Existing Commitments for Democratic Elections in OSCE Participating States: A Progress Report*, which identifies potential issues raised by the implementation of new technologies in the election process. The report was welcomed by 2003 OSCE Ministerial Council Decision (MC 05/03), which tasked the OSCE Permanent Council to consider the need for additional commitments on elections, drawing on expertise from the ODIHR;

2) the 2005 OSCE Ministerial Council Decision (MC17/05) tasking the ODIHR to submit a report on implementation of existing commitments, possible supplementary commitments, ways of strengthening and furthering its election-related activities, and improving the effectiveness of its assistance to participating States;

3) the ODIHR's 2006 report *Common Responsibility* which stated that the ODIHR would make efforts to "further refine the methodology as necessary… to meet new and emerging challenges, especially new voting technologies" and to "develop a stronger capacity on the use of information technology and on the observation of electronic voting", and identified "perceived and real challenges to transparent and accountable elections that have arisen in the context of new voting technologies" as an issue for discussion in the context of possible supplementary commitments;

4) the 2006 OSCE Ministerial Council Decision (MC 19/06) which agreed "that ODIHR should put into practice the improvements and recommendations concerning election related activities, including as contained in the [*Common Responsibility*] report," and specifically called on ODIHR to further strengthen its observation methodology.

In addition, the OSCE has conducted two Supplementary Human Dimension Meetings dealing with issues related to the use of new technologies in elections: in July 2004 on *"Electoral Standards and Commitments"* and in April 2005 on "*Challenges of Election Technologies and Procedures."* Following the 2005 meeting, the OSCE Chairmanship issued a *Non-Paper on the Challenges of Election Technologies and Procedures* in which it proposed that ODIHR call "a meeting of experts to discuss the relevant issues related to automated or electronic voting, with the aim to develop Guidelines on observation of such new election technologies." ODIHR organized two expert meetings, in October 2006 and March 2007, which led to the development of this Discussion Paper.

II. DEFINING ELECTRONIC VOTING

The term "electronic voting" is intended to be construed broadly, encompassing any technology for casting, counting, or tabulating a voter's electoral choice by electronic means. As with traditional paper voting, electronic voting can be conducted in a controlled environment, such as polling stations, or remotely in an uncontrolled environment.

The more widely known electronic technologies used in polling stations are:

(1) optical scan systems that electronically record a vote from a special paper ballot marked by the voter, and
(2) direct recording electronic voting systems ("DRE"), such as a touch-screen voting, which may or may not include a paper record of the vote cast.

DREs currently in use can be divided into three main categories:

- Touch-screen voting systems with a paper record retained by the system that provides for voter verification of the paper record before the vote is actually cast (voter-verified auditable paper record or VVAPR);
- Touch-screen voting systems without a VVAPR; and
- Push-button devices, where the voter presses one or more buttons next to the candidates of his or her choice, and then presses a "vote" button.

Of the DRE equipment, only those with VVAPR systems offer a manual recount facility. Other DRE systems rely on the built-in memory when a recount is undertaken and are only able to produce an exact copy of the original reported outcome. These systems store their record of ballots[8] cast in separate hardware, such as a hard disk or a memory card, and most keep a log of all operations (audit log). Inspection of this data may clarify matters if a recount is needed, but this requires the intervention of an expert and that there be no hardware failure.

Optical scan technology uses a special ballot paper that is marked by a voter, inserted into a scanning device, and counted by the device reading the voter's mark on the ballot. However, the ability of such devices to scan the voter's choice depends on the voter marking the ballot properly, and is subject to the devices' intrinsic margin of error. Optical scan technology offers the possibility of a manual recount facility.

The internet is the primary voting channel currently in use in remote electronic voting, although it is also under consideration in some countries for use in controlled environments. While the internet offers potential advantages in increasing accessibility, it can create additional challenges in ensuring the secrecy of the vote, in ensuring that votes are counted as cast, and in ensuring that the integrity of the process is secure. In addition,

[8] It is important to make a distinction between the "ballot display", which is what appears on a screen in front of the voter, and "ballot of record", which will be either a cast paper ballot that is printed or cast ballot image that is recorded electronically. "Cast" means reflecting the voting preference indicated by the voter.

an outstanding concern is that internet voting systems currently offer no possibility for a meaningful manual recount of votes.

The above systems are not the only types of electronic voting systems. There are other systems where the casting, counting, or tabulation of the voter's electoral choice is done by software and hardware instead of people, pen, and paper.

III. EXISTING STANDARDS FOR ELECTRONIC VOTING SYSTEMS

Within the last few years there has been a concerted effort to develop standards for electronic voting systems. In 2004, the Committee of Ministers of the Council of Europe issued its Recommendation on Legal, Operational and Technical Standards for E-Voting.[9] This Council of Europe Recommendation followed a report of the European Commission for Democracy through Law (Venice Commission) concerning the compatibility of remote and electronic voting with the requirements of Council of Europe documents.[10] The Election Assistance Commission of the United States, with assistance from the National Institute of Standards and Technology of the Department of Commerce, developed Voluntary Voting System Guidelines in 2005. These guidelines were in the process of being updated in October 2008.[11]

The development of these standards constitutes progress for assessing electronic voting systems. The Council of Europe Recommendation on Legal, Operational and Technical Standards for E-Voting recognizes the importance of ensuring that electronic voting processes are observable. However, the above standards are technical in nature,[12] emphasizing some aspects of electronic voting that may exceed the scope of an election observation or assessment mission. A simpler and more basic guideline of considerations for the observation or assessment of electronic voting is needed for the OSCE/ODIHR.

IV. CONSIDERATIONS FOR OBSERVATION OF ELECTRONIC VOTING

The OSCE/ODIHR EOM[13] should, similar to its methodology for observation of traditional voting systems, base its conclusions on information obtained from a rational and consistent methodology. This requires differentiating between what can be realistically observed and what cannot. Some components of electronic voting simply cannot be observed by an EOM. However, there are aspects of electronic voting that can be observed

---

9 Adopted by the Committee of Ministers of the Council of Europe on 30 September 2004; www.coe.int/t/e/integrated%5Fprojects/democracy/02%5FActivities/02%5Fe%2Dvoting/

10 Report on the Compatibility of Remote Voting and Electronic Voting with the Standards of the Council of Europe, The Venice Commission, 18 March 2004; http://venice.coe.int/docs/2004/CDL-AD(2004)012-e.asp

11 The Voluntary Voting System Guidelines are available at www.eac.gov/vvsg

12 The Association for Computing Machinery (ACM) has formulated a brief recommendation, stated in less technical language, for integrity, security, and usability in electronic voting. *See* ACM recommendation and statement on e-voting, 28 September 2004, www.acm.org/usacm/weblog/index.php?p=73

13 Throughout the text, the term "EOM" also encompasses the term "EAM" unless otherwise noted.

and sound conclusions about an electronic voting system in general can be reached.

There are several areas that the EOM should consider when observing electronic voting,[14] including the following: (1) background leading to the decision for electronic voting and comparison with the system being replaced; (2) the legal framework; (3) how the particular electronic voting system was chosen; (4) certification and testing of the system; (5) secrecy of the ballot; (6) security of the entire system and its functioning; (7) voter accessibility and education; (8) analysis of documentation relevant to the system; (9) election administration and training of polling station officials in operating the voting system; (10) overall transparency and public confidence; (11) audits of the system; and (12) recounts and challenges to results.

Two considerations which are not separately listed above, but which are implicit in all areas, are accountability and rationality. Individuals and legal entities involved in the implementation of electronic voting, including vendors, must be held accountable for their actions, conduct, and decisions, and no exemption for culpability should be given because a new technology is involved. There must be clearly defined responsibilities and legal consequences for misconduct and negligence in the implementation of electronic voting just as there are for traditional voting systems. Secondly, designs and decisions must be driven by rationality. Any chosen solution must have a direct relationship with the desired goal.

A. BACKGROUND OF DECISION FOR ELECTRONIC VOTING AND EXISTING SYSTEM COMPARISON

Electronic voting is never introduced in a vacuum. There are reasons that a country makes changes in any of its electoral processes, whether it be the formula for allocating mandates, the legal threshold for participating in mandate allocation, or deadlines for filing complaints challenging election results. The EOM should consider the background leading to the decision for electronic voting.

Although the general benefits associated with electronic voting may be stated by some interlocutors, additional inquiries should be made by the EOM to assess to what extent the introduction of new technologies may be politically and/or economically motivated. The EOM should consider the full background leading to the decision for electronic voting. The EOM would also seek information on whether such a change would negatively impact the ability of voters from minority communities to elect representatives.

The EOM should also consider the process leading to the decision to implement the electronic voting system. Was the decision made after the public, civil society groups, and political parties had the opportunity to comment and share their views? Was the decision made hastily or after a sufficient period of public discussion? Was the decision to implement an electronic voting system reached by political forces by consensus or broad

[14] An initial step toward the establishment of an OSCE/ODIHR EOM is the deployment of a Needs Assessment Mission (NAM) before a given election. The NAM should be able to identify areas of priority and determine the nature of the electronic voting expertise that will be needed on the core team of the EOM.

agreement? If not, how significant was the opposition to it? Were representatives of the academic and election administrators' communities consulted and what were their views?

Opposition to the implementation of electronic voting may be an indication of a lack of public trust in electronic voting in the country. This mistrust may remain regardless of what efforts are made to interject full transparency and observation as an element of the electronic voting system. Lost public confidence can be difficult to recover.

One of the most important aspects in the analysis of the decision for electronic voting is a general comparison of the electronic system with the voting system that is being replaced. Does the electronic voting system command the same level of confidence as the system it is replacing? In simplest terms, does the electronic voting system ensure secrecy of the ballot while at the same time providing for at least the same degree of accuracy, audit (recount) capacity, and transparency as the system being replaced? An electronic voting system should be able to achieve a high degree of accuracy as it is generally considered that it could be a remedy for simple human error. Secrecy of the ballot, audit and recount capacity, and transparency are more challenging areas in an electronic voting system, but these are fundamental tenets of a democratic election process and must be upheld.

B. THE LEGAL FRAMEWORK

The conduct of democratic elections is a responsibility, first and foremost, of the public authorities. Electronic voting raises legal issues, particularly regarding codification of election procedures. The law or other binding regulation must correctly and precisely incorporate technological processes into legal text that is transparent, objective, and capable of being applied to address all situations that may arise. This is difficult enough when regulating traditional paper ballot elections. The legal framework for the electronic voting system should be developed first to prescribe the requirements for such a system and not as an afterthought once a system is in place for elections. This means that vendors should implement the requirements of the public authorities rather than vice-versa. Transparency, accountability and public confidence take priority over any interest of vendors or certification agencies.

A fundamental issue the law should address is how the electronic voting system can ensure that votes are counted as cast. If the electronic voting system:

(1) produces a voter verifiable auditable paper record (VVAPR) that the voter can view before leaving the voting booth in order to ensure that the voter's choice has been recorded accurately; and

(2) if, after this, the VVAPR is retained in a container preserving the secrecy of the vote and stored there like traditional paper ballots for use in possible audits and recounts;

then it could be considered that the system provides for safeguards that adequately ensure that this fundamental principle is implemented. Respect for this fundamental principle can further be enhanced if the law requires that mandatory audits, in a set percentage of randomly selected polling stations, be conducted as a standard practice after the voting.

The requirement in the legal framework for the use of paper as the key and controlling element of electronic voting cannot be avoided. The law must ensure a paper record so that a voter can verify the accuracy of his or her vote, and to create an independent check on the electronic result produced by the electronic voting system. Speed and ease for vote tabulation is "no substitute for accuracy of results and trust" in the electoral process.[15] This also requires that the law mandate that the paper component of the system maintain some degree of permanency in order to allow for audits and recounts and that the law address the issue of whether paper or electronic records prevail in the event of discrepancies.

One of the most difficult challenges faced in developing legal text is the issue of how much detail to require on the issue of transparency of the electronic voting system. There are different opinions about how access to electronic voting systems should be presented in legislation – whether the principle of full access should be included, or specific aspects that are necessary for a "minimum level of transparency" should be stated. Additionally, the components of electronic voting systems may be too diverse to specify exactly what kind of observer access is required.

Another issue raised is the definition of the shares of responsibility and the legal accountability of vendors, certification institutions and election administration for the electronic voting system. Legislation should carefully regulate the responsibility of vendors in order to ensure that there are no grey areas in which vendors could possibly usurp responsibilities vested in public authorities, and furthermore that there are consequences for failure to fulfill contractual obligations related to electronic voting. Similarly, certification agencies and election administrators must be held strictly accountable in order to ensure that they fulfill their respective public responsibilities.

Some of the specific areas that should be addressed in legislation regulating electronic voting include:

- The consequences of technological failure of electronic voting equipment in one or more polling stations and/or electoral districts;
- The scope of access that will be afforded to observers;
- The procedural steps for audits and recounts;
- The primacy of the VVAPR in determining the results in the event of discrepancies or legal challenges;
- Defining the contractual obligations of vendors, suppliers and certification agencies; and
- Accountability provisions for public officials and election administration.

Legal accountability for election officials is an important element of the legal framework. Greater responsibility is placed on election officials working in systems with electronic voting because they are additionally charged with the responsibility for the product delivered by the vendor and certified by the certification agency. While the election authorities should be responsible for the overall conduct of an election, including the performance of any technologies used in the election process, contractual issues should be considered carefully to determine the degree of responsibility that vendors and certification

[15] Op. cit., ACM Statement on E-voting.

agencies should have for the supplied product. This is necessary since their respective roles in electronic voting are greater than in traditional voting.

C. HOW THE PARTICULAR ELECTRONIC VOTING SYSTEM WAS CHOSEN

There are different types of electronic voting systems and various vendors promoting, developing and selling them. Although an EOM does not determine whether the "best" type of system was chosen, it may wish to consider the process by which a particular system was chosen. Criteria used for selecting a particular type of system should be clearly established in advance of selection and made available publicly. This includes not only technical criteria but also purchasing and procurement criteria.

It is also important to consider how the specific vendor of the electronic voting system was chosen. In addition to meeting technical and procurement requirements, did the selected vendor have prior experience with electronic systems used in elections? Has that prior experience been positive or negative?

An important factor to consider for the selection process is the overall transparency of the process. When all stages and phases of the process are viewed as a whole, was the process transparent and subject to public scrutiny? Was the selection process sufficiently open so that all vendors had the opportunity to participate? Or, does it appear that the process was "tailored" for a particular vendor? These are important matters to consider when assessing the overall transparency of the selection process.

D. CERTIFICATION OF THE SYSTEM

Certification is a process to establish whether a given electronic voting system satisfies previously established standards and legal requirements. It is not the function of the EOM to certify a particular electronic voting system used in a country. It is the responsibility of the public administration in the country to ensure that the electronic voting system has been properly certified before it is used in elections. However, the EOM should assess the certification process that was used. In order to do this, the EOM, as well as domestic observers, should have maximum access to the documentation on the certification process.[16]

Observers should try to establish whether certification requirements existed prior to the introduction of the electronic voting system. They should also determine if the standards were public and in accordance with the relevant legal provisions. Observers should try to determine how specific the standards are and to what extent the certifying body has a certain latitude in assessing compliance with the requirements. The EOM should consider whether there are any potential gaps in the certification criteria. In doing so, the EOM should also try to establish contacts with the domestic academic community and seek their opinion about the electronic voting system and the certification process.

---

[16] It is possible that there is no certifying body in a country where there is only one type of electronic voting system available or the election administration has developed its own system. This should be noted by the EOM. The issue of system testing remains particularly important in the absence of a certification process.

Certification of the system, both software and hardware, should be performed by an expert body independent from vendors, suppliers and election administrators. Since part of the certification process is the certifying body itself, information on the certifying body is relevant for the EOM. The EOM should attempt to determine the prior experience of the certifying body, whether the certifying body is truly independent in the above context, and whether the certifying body is itself accredited, in order for certification to be meaningful. An indicator for this is the source of funding for the certification process.

It is helpful if the EOM can obtain public information that is available on the certifying body. This includes prior certification experience, whether the certifying body has experience in more than one country, and a range of opinions of election administrators who have relied on the certification body. A problem the EOM may encounter is establishing to a reasonable degree of satisfaction that the certifying body is indeed what it is purported to be. It may be the case that a truly independent certifying body does not exist.

Consideration should also be given to how the certifying body conducted the certification process, including the steps, personnel, and amount of time devoted to the certification process. Was the process a meaningful one or mere "rubberstamp" approval? Were any modifications made to the system's hardware or software subsequent to the original certification? If so, were these modifications certified? What remuneration was paid to the certification body if relevant? Was this amount sufficient for a meaningful certification process or obviously inadequate to include more than a brief look at the system?

E. TESTING OF THE SYSTEM

In addition to certification, the EOM should attempt to determine to what extent the system has been subjected to testing and to what extent the testing process is fully independent, transparent, and comprehensive.

Since testing generally happens before the EOM is deployed, documents related to testing should be available to the EOM. The EOM may determine that discussions with "testers" are necessary to answer questions not resolved by documentation. This may include vendors, certification agencies, election administrators, or any group, such as candidates, political parties, academic institutions or civil society groups that was permitted to engage in additional testing.

Degrees and phases of testing should be considered by the EOM. This includes documentation on the testing done in the laboratory for the purpose of seeing whether the system or components of the system meet design criteria and whether all parts of the system function together as designed. Observers should attempt to determine whether the results of testing were made available to political parties and civil society.

Observers should consider the extent of testing of the system with voters, possibly in pilots or trials. This tests not only the electronic voting system, but also the user friendliness of the system as well as the sufficiency of voter training and education. Further, testing should continue after use in elections and on a regular basis to ensure that the system

continues to work properly, particularly after installation of upgraded or new software.

The EOM should consider to what extent candidates, political parties, and other groups were permitted to test the electronic voting system. Obviously, such testing may be limited as technical, security, logistical, and time constraints prevent the possibility of complete or renewed testing beyond the initial testing required by election administrators before the system is accepted for use in elections.

Regardless of the degree of additional testing that the election administration permits to be conducted by other persons and groups, election administration must ensure that the system has been completely tested before it is used. This includes "end-to-end" testing as well as testing of individual components. Election administration must also ensure that there is complete and full documentation establishing that the system has been adequately tested. Use of an electronic voting system in elections, where it has not been fully tested or for which there is insufficient documentation of such testing, risks jeopardizing the legitimacy of the election process.

It is important to note that international observers should not be involved in certifying or conducting testing of any systems or devices. It should also be noted that testing is no guarantee that the electronic voting system is secure and working properly. The value of testing depends in part on the type of testing and by whom it is done.

F. SECRECY OF THE BALLOT

Secrecy of the ballot is a fundamental principle enshrined in OSCE commitments that must be respected regardless of the voting system used. A voter must have assurance that the voter's electoral choice will not be disclosed to anyone. Not only must the voter be able to mark the ballot in privacy, the system must also ensure that the voter cannot be associated with his or her choice.

While ensuring secrecy of the ballot in the polling station is similar to guaranteeing a secret place to vote in a traditional system, it also is a technical question where voting is done by an electronic system. Observers must assess to what extent safeguards are in place to ensure secrecy of the ballot and must assess the effectiveness of those safeguards. Ensuring that safeguards are in place requires examination of the documentation reflecting the design, testing, and certification of the system. Observers should establish how anonymity is accomplished in the design of the system. Other elements of secrecy of the vote include assessing the physical layout of the polling station and whether touch voting screens can be seen by other persons while a voter is making his or her choice on the screen. It also requires consideration of technical issues such as whether electronic events in the voting equipment can be intercepted or read by third party devices.

Concerns with secrecy may arise based on the procedures used for voting. The brightness and the size of some computer screens may make voter choices visible to others if the machines are not oriented correctly. Importantly, the voter should not be able to retain any piece of paper or other evidence that can later be used as proof of how the voter has voted. As an example, if a voter is able to retain a confirmation code for the purpose of matching the voter's cast ballot with the code later, then the voting procedure itself raises a concern

with secrecy of the ballot.

Remote electronic voting, including internet voting, raises additional problems for ensuring secrecy of the ballot. There are no absolute safeguards to ensure secrecy in an uncontrolled environment. As with postal voting, secrecy of the ballot becomes a difficult challenge where electronic voting is conducted remotely, such as with internet voting or other systems. In addition, remote electronic voting requires sufficient encryption in order to ensure that if the transmission of the vote is intercepted by a third party, it will not be possible to determine the content of the vote. Observer missions should have the capacity to assess the extent to which effective safeguards are in place where remote electronic voting is in use.

G. SECURITY

All components of the electronic voting system, including equipment, premises, and data, should be secure at all times. It is very important to maintain security of all data that is electronically processed or stored. The electronic voting system should be secure from external attack or attempts to decipher information, internal manipulation, and technological failure. Overall, observers should identify whether appropriate safeguards are in place to prevent or detect illegitimate interventions in the system.

Physical and electronic access to the electronic voting system must be strictly regulated by written procedures.[17] Physical and electronic access to the system should be limited so that an election worker or vendor has access only to components that necessarily come within the performance of his or her duties. The performance of sensitive system operations should be performed by more than one person in order to avoid internal manipulation by one person. There should be a division of duties within election administration to minimize the opportunity for internal manipulation. Further, these operations should be subject to observation by candidates, political parties, and observer groups. Observers should also check who has official access to the system and under what circumstances. A written record of all operations performed should be maintained and all audit logs preserved.

External manipulation – "hacking" – is a significant risk but one which may be decreased if different levels of security in the system make hacking difficult. Internet voting or the linkage of any system with external networks, however, increases the risk of the system being hacked. Measures should be in place to ensure that attempts at external manipulation and/or attempts to decipher information can be detected, reported and prevented.

Security of a system can be observed by focusing on processes of data entry and the steps involving programming of the system. However, the latter might give rise to objections from a vendor or electoral authorities that assert that such observation is precluded by intellectual property or copyright law. Other observation procedures may include examination of the management guidelines regulating the programming of the system. This can include a list of personnel and dates and times of programming and other

[17] Security can also be enhanced if written rules specify what a system of electronic voting must not do.

electronic interventions in the system. Transport of software and equipment to polling stations should be considered as well as the controls in place during these operations. Other queries are also appropriate. Where are the entry points to the system? When does software or equipment leave the controlled environment? When was software loaded? Who has access if new input is needed for the system? Is the software source code made public or available for inspection by candidates, political parties or independent bodies? Is there an independent body which analyses the software before and after the election to certify that it has not been changed?

Assessment of security issues requires examination of reports and documents and requires the observer mission to have specific expertise in this area. However, there are some areas of security that can be considered as they would be in a paper system, such as the use of serial numbers for voting equipment, chain of custody forms, and logs for access to secured premises.

H. VOTER ACCESSIBILITY AND EDUCATION

There are number of areas in which an EOM can make assessments regarding accessibility of the electronic voting system for voters and the provision of voter education. The electronic voting system should be understood and easily used by voters. The system design should take into account the level of education and computer literacy in the country and the existence of similar systems used by the populace for other purposes.

An electronic voting system should facilitate voting by voters with special needs. Consideration should also be given as to whether a voter may use the electronic voting system in a minority language. Where it is possible to vote in a minority language, it should be verified that the minority language ballot contains the same information as regular ballot.

Generally, to the extent possible, principles for the design of paper ballots should also apply to electronic voting. The EOM should consider to what extent candidates are presented equally on the ballot and whether all information required by law is presented. All candidates or parties contesting the election should be given an equal amount of space on the electronic ballot and have been seen on the screen before the voter votes. This should be taken into account when designing the electronic voting system and providing voter education. This may present a problem, however, with internet voting, since the screen display will vary in the homes of many voters.

Ballot design is a distinct component of the electronic voting system. Ballot design is determined in part by the registration of candidates and the registration process may not be concluded until a matter of weeks before the election. After candidate registration is concluded and the election administration has determined the electronic ballot format, the EOM should assess whether voters may experience any difficulty in voting due to the ballot format. This is also important for the briefing of short term observers in order to anticipate potential problems on election day.

The step during which the vote is finally cast should be clear to the voter. Until that moment, the system should provide a voter the opportunity to review the selection and to

change his or her choice. It is important to provide this information to the voter during the voting process. In a paper voting system, this information is generally known by voters since voters understand that applying a pen to the surface of paper will generate a mark for the voter's preference and that depositing the ballot paper in the ballot box marks the final step of the voting process. In an electronic voting system, the steps for voting should be clearly explained to the voter during the voting process.

Voter education is critical for the implementation and use of an electronic voting system. Observers should assess the extent to which information about the system has been made available to voters and the completeness of this information, particularly when a new system is being implemented or where significant modifications have been made to an existing system.

Voters themselves should be one of the components of security, since elections belong to voters, and they will often be the first to notice any problems with a given machine. A voter should know when the electronic system is not working properly during the voter's use. This requires voter education on not only how to cast the ballot electronically, but also on how the electronic voting system should perform during the voting process. Voters should also be educated on the security measures introduced to protect the system.

An electronic voting system should be tested publicly by the voters themselves in a series of trials to determine whether the system is user friendly. Such trials will also help to identify any problems or shortcomings that may exist in the electronic voting system. Election day should not be the first occasion where a voter has the opportunity to become familiar with and use the electronic voting system.

I. ANALYSIS OF DOCUMENTATION RELEVANT TO THE SYSTEM

Physical observation of all aspects of electronic voting is not achievable. Thus, there must be a thorough examination of the documentation relevant to the system.[18] Selection, certification and testing of the electronic voting system will likely occur prior to the EOM's arrival. Observation is limited, to a degree, to analysis of documents and assessment of public trust in the process. The EOM's observation of the electronic voting system should include assessment of the procedures around the system, including procurement, certification, testing, and audit mechanisms.

Given the large amount of documentation regarding the technical specifications of the system, certification, testing, and security, as well as the need in some cases to translate the documentation, the OSCE/ODIHR should request the documentation prior to the deployment of the EOM. It may on occasion be advisable to include an electronic voting expert in the initial OSCE/ODIHR Needs Assessment Mission in order to identify the documentation that will be needed.

An important element of document examination is identifying the absence of documents. The existence of relevant documentation is not conclusive regarding the reliability of the

[18] Meetings and discussions with interlocutors are also important as valuable information can be obtained in interviews as well as through examination of written documentation.

electronic voting system. However, the absence of relevant documentation may be an indication of problems. The absence of documentation for dealing with known technological problems may be more relevant than the documentation that is available for examination. In short, missing documentation may be more important than available documentation in the EOM's overall analysis.

J. ELECTION ADMINISTRATION AND TRAINING OF POLLING STATION OFFICIALS

An important element of any election system is the election administration. Assessment of an electronic voting system is partially an assessment of the election administration. Any failing by the election administration may influence public confidence in the overall election process as well as in the electronic voting system itself.

One element of the assessment of the election administration is the nature of the election administration's relationship with vendors and degree of dependence on vendors for administration of the election. It should be determined if there is a level of expertise within the election administration to address problems that might be encountered during electronic voting without relying on vendors. Further, where temporary personnel are hired by the election administration as internal experts to deal with problems, the relationships and links that these temporary personnel have with vendors should also be considered. Significant reliance on outside sources, even on a temporary basis, can minimize the impartiality and independence of the election administration.

Where there is a significant degree of reliance on vendors, observers should inquire further to assess if this reliance has fundamentally altered the ability of the election administration to control implementation of voting processes. If the voting machines are programmed by vendors and the source code is secret, then the election administration has limited access and control. This requires the machines to be re-programmed before each election by the vendor. The vendor has effective access to the results and the election administration is marginalized.

A prudent election administration assumes that the electronic voting system, due to either technological complexity or human factors, may fail. The EOM should assess what contingency planning has been taken by the election administration. What post installation safeguards and contingency plans have been introduced to address possible system failures? How will electronic data be preserved and recovered in the event of a physical failure, such as a loss of power? Who is responsible for fixing the problem and in what response time? Is there a manual for polling staff to detect failures and which steps to take in such cases? Is there a possibility to continue voting by paper ballot once a failure has occurred? In case of a failure, there should be clear guidelines on the respective responsibilities of vendors, certification bodies and election administrators to fully ensure accountability and an effective response. Anytime something happens in the polling station related to the electronic system (*e.g.*, if the system fails, functions abnormally, or if procedures regarding the operation of the system are not followed properly), the incident should be written down, recorded and signed.

Some of these issues can be assessed more readily because visible systems should be in place, such as UPS (uninterruptible power supply) systems in polling stations in case of

power failures, or instruction manuals in the polling stations and relevant election commissions. Questions about how the system has been designed to address failures can be asked by the core team's electronic voting expert, while long and short term observers can also enquire about contingency plans, manuals, training, and other issues related to procedures.

Observers should also look at the liability and responsibility of vendors and suppliers. Whether codified in law or reflected in the written agreement with the vendor, there should exist on the part of the vendor the continuing responsibility to maintain and service the system. This is an element that can be verified by observers.

Training of election administration is critical for the conduct of electronic voting. Electronic voting presents greater challenges and burdens than paper voting systems. As a result, more training must be provided to election workers. Election workers must be able to assist voters as well as respond to minor problems and major emergencies. This requires that election workers must have some basic understanding of how the electronic voting system works, not only in order to respond, but to reassure and instill confidence of voters in the system. A certificate or exam for system operators may be advisable. Without qualified and trained election workers, the risk of dependence on vendors for administering elections becomes greater. Elections should be administered by public authority institutions and not outsourced to the private sector.

The EOM should, where it is possible, observe training of polling officials and review training materials to obtain a better understanding of the electronic voting processes. This can be particularly valuable in the briefing of short term observers. It can also reveal shortcomings in training and potential election day problems of which observers should be aware. Where the election administration relies on vendors to administer the electronic voting process, or where they have a significant role in the process, then the training of the vendor's employees becomes relevant. In such a situation the vendor and its employees are performing *de facto* election administration responsibilities, and should be held accountable as appropriate.

In addition, the role of vendors and their responsibility in providing training should be considered. However, ultimate responsibility for ensuring that election officials at all levels are appropriately trained is vested with the public authorities accountable for the conduct of democratic elections.

In systems in which electronic voting systems are used together with paper voting systems, it may be necessary for observers to assess how these processes interface, for example in management of the voter register, polling station procedures, or in the tabulation of the votes.

K. OVERALL TRANSPARENCY AND PUBLIC CONFIDENCE

It is an accepted principle that observers should have the right to inspect documents, attend meetings, and observe election activities at all levels, and to obtain copies of decisions, protocols, tabulations, minutes, and other documents, at all levels, during the entirety of the election processes, including before and after election day. The basic premise is that

every element of the electoral process must be open to full and complete observation. One of the reasons for complete transparency is that it is necessary for ensuring that the elections are genuinely democratic and that the votes have been accurately counted and honestly reported.

Transparency considerations require that observers have access to the electronic voting system. However, access must be balanced in order to respect the principle of non-interference with the administration of the election. Inappropriate access may also result in damage to the system, such as compromising the security of the system. This is why certification, testing and security of electronic systems, and examination of documentation related to certification, testing and security, must be readily available for observers.

As noted above, it might not be feasible for domestic observers, political contestants, or other persons outside of election administration to test the system in its entirety. However, they should have the opportunity to run specific tests or audits to check the functionality of the system. They should also have the opportunity to become familiar with the database management, procedures, maintenance, and updating processes for the system. This requires that the election administration develop procedures for translating the principle of access for observers into practice without impeding the administration of elections or harming the system.

Overall transparency can be enhanced by different factors. Where any component or process of the system is secret or protected from disclosure by law, then overall transparency decreases. As elections are a public process exercised collectively by voters in order to realize basic human rights, the electronic voting system should not be made secret by a private agreement between a vendor and the election administration. Elections are not for vendors or the election administration; elections belong to the voters.

One factor that impacts overall transparency is the issue of source codes for the software that operates the electronic voting system. Where the source code is a matter of public information and easily viewed, then overall transparency is enhanced. The source codes for all software used in the electronic voting system should be made public. However, making open source codes public may be of limited value unless the public has the possibility to check if this source code, or better, the resulting compiled software, is actually present in the voting system. The electronic voting system should be sufficiently transparent to allow persons, other than only the vendor and election administration, access to all information relevant for addressing and correcting problems and malfunctions.

Where electronic voting occurs in a polling station on a device such as a DRE, transparency can be enhanced if there is the fundamental requirement of a paper record for each ballot that has been cast. Observers should assess whether there are facilities that produce a permanent paper record of votes cast with a manual audit capacity and under what circumstances audits of the results must be conducted. Observers should check whether such records are voter verified.

A paper record requirement must be implemented properly to achieve the goals of transparency and public confidence. Technical issues, such as the type of paper, storage,

printing, cutting, and deposit of paper in the ballot box, significantly impact the effectiveness of the paper record. The voter must be able to physically see and read the paper record of the vote before leaving the polling booth. This requires that the paper record not be a bar code or contain information that is indecipherable to the voter. A paper record must also be of sufficient quality to permit a recount or audit where legally required. Illegible paper records are of no value.

Although a paper record can enhance transparency, it must be implemented in a manner that preserves the secrecy of the ballot. The voter should not be able to retain any piece of paper that can later be used as proof of how the voter has voted. Thus, a paper record can only be used in the controlled environment of a polling station. A paper record would not be a viable option for internet voting.[19]

Polling stations and higher levels of election bodies should produce paper protocols of their result tabulations so that political parties, candidates, and observers can check that the results at lower levels can be verified against the centrally recorded electronic voting results. The EOM should ascertain whether this is in fact a requirement.

The EOM should also consider to what extent political parties and domestic non-partisan organizations utilize possibilities for access to electronic voting systems and documentation afforded to them during the election process. Have these observers requested access? If so, what checks were they able to perform and is there information that they were unable to obtain? If not, was this due to legal restrictions, lack of expertise, overall trust in the election administration, or other reasons?

L. AUDITS OF THE SYSTEM

Mechanisms for audits are important considerations for observers. Audits may be of different types, including audits of the functioning of the voting machines and audits of the procedures followed in administering and securing the system, as well as audits of the results. If conducted independently, these procedures may alleviate many of the concerns that arise from the inability to view with the naked eye the electronic events taking place in the "black box" of the electronic voting system. Domestic observers and representatives of political parties, candidates, and the media should be allowed to be present during audits.

The possibility for a voter to verify his or her vote through a paper record, at the time of casting the ballot, is an important and positive feature in facilitating audits, as it allows eventual audits of results to compare paper and electronic results.

A procedure for mandatory audits to determine whether the electronic voting system has reported the results properly can also build confidence in the system. Observers should determine whether there are provisions for mandatory random audits of the voting results in some polling stations. The voter verified paper record in a statistically significant percentage of polling stations should be randomly selected for a manual recount, in order to confirm that the electronic voting results are accurate. The law should be clear on the manner in which the random sample for an audit is determined and whether observers,

[19] Internet voting would require an electronic solution for verification of the voter's vote.

candidates, or political parties have the right to designate a minimum number of polling stations to be included in the audit.

The law should be clear what additional action is required should a mandatory audit or recount reveal discrepancies and what affect, if any, it has on the results. An audit requirement is of little value if it does not necessitate some form of corrective action – either of the results or the electronic voting system – should the audit reveal discrepancies. In fact, without a requirement for some corrective action, the audit could create more problems than solutions. An audit requirement should be intended to safeguard the system and, where there is a problem, to correct and improve it. There should not be an audit requirement merely to provide a sense that the system is working.

Observers should check whether audit mechanisms provide relevant information for all levels of the electronic voting system, from the specific voting device to tabulation in the polling station and on through later tabulations in higher election commissions. Observers should check that audit mechanisms preserve the secrecy of the ballot. However, ballots cast electronically must be stored individually and preserved in a paper record in order for an audit or recount to be possible.

M. RECOUNTS AND CHALLENGES TO RESULTS

In order to ensure that votes are counted honestly and the results are reported accurately, it is necessary that mechanisms be in place for an opportunity to recount the votes where justified by the circumstances. One example would be where a known election system failure, that could have affected the results, is brought to the attention of the election administration. Another example is where the margin of victory is narrow. The legal framework should provide the possibility of a meaningful manual recount of ballots cast electronically.[20]

In the case of a discrepancy between the paper record and the electronic record, the law should clearly state how the discrepancy affects the results and whether any portion of the results must be invalidated. Although the paper record is generated by the electronic voting system and the two results should be the same, system flaws, printer malfunctions or intentional malfeasance might result in a situation where the two are not the same. The legal framework regulating challenges to election results should address the issue of whether paper or electronic records prevail in the event of legal disputes

N. REMOTE ELECTRONIC VOTING

Voting systems that involve casting a ballot in a remote, unsupervised location by electronic means, such as by internet, mobile phone or other devices, present special challenges to the integrity of an election process. In addition to the challenge to ensuring the secrecy of the vote presented by other forms of remote voting (e.g., postal voting), remote electronic voting raises issues regarding safeguards against potential violations of the integrity of the voting process, denial of voting rights through external attacks, the

[20] Internet voting, again, presents unique issues. A recount of votes cast electronically from outside of the controlled environment of the polling station may be a significant technological challenge.

security of the devices used by voters to cast their votes,[21] and the inability of voters to be certain that votes are counted as cast.

Remote electronic voting has some perceived advantages, particularly in expanding accessibility to voters who may not be able to go to a polling station, and there have been efforts to define standards for its use, notably the 2004 "Recommendation on Legal, Operational and Technical Standards for E-Voting" of the Committee of Ministers of the Council of Europe. Nevertheless, the challenges to the conduct of a transparent election process that enjoys broad public confidence and the associated risks of failure may be too great at present to make remote electronic voting systems suitable for general use, especially in national level elections.

An EOM that must assess remote electronic voting as part of its tasks can consider a number of elements of the process. These elements include the certification and testing of the system; the legislative framework; security measures implemented to protect the system from internal manipulation, external attack, and system error; the adherence to procedures by the election administration, vendors, and other entities involved in the system; the accountability of these bodies and individuals; the access of political parties and other domestic observers to documentation and to the functioning of the system, including the source code; the conduct of audits; and the overall confidence of voters, political parties, and civil society in the process. The OSCE/ODIHR should therefore include in its guidelines specific considerations for the observation of remote electronic voting.

However, the EOM would unlikely be able to observe the voting process itself in an effective manner and may be unable to reach conclusions about the integrity of the process and its adherence to fundamental democratic principles, due to the inherent lack of transparency in remote electronic voting. These considerations should also be reflected in the eventual OSCE/ODIHR guidelines.

V. RECOMMENDATIONS

Many issues are presented to election observers where the election processes involve some element of electronic voting, either through the casting, counting, or tabulation of ballots. In light of the discussion above, recommendations are made for three areas in order to improve observation of electronic voting: (1) core team composition; (2) role of short term observers; and (3) development of fundamental safeguards for transparency and public confidence for electronic voting.

---

[21] An internet voting system that would allow voting from home on a voter's personal computer could be problematic in a number of aspects. In addition to secrecy issues related to voting in an uncontrolled environment, personal computers in the homes of individuals could be infected with spyware and not secured from possible attacks or violations of the secrecy of the vote. Further, there may be considerations as to whether each potential voter will have on his or her computer the necessary hardware and software and will be able to verify that it is functioning as it supposed to. There can also be problems should there be power cuts or internet disruptions at the time of voting.

A. CORE TEAM COMPOSITION

Electronic voting is a complex technology that is not easily understood by the average person. Thus, it becomes necessary to have as part of the core team a qualified expert who can advise the OSCE/ODIHR EOM on electronic voting issues and provide guidance for long and short term observers for this element of the observation. Given the scope of issues to be considered, best practice would be that an EOM include more than one such expert in the team, in order to achieve a diversity of opinion.

As with other core team experts, the electronic voting expert(s) should be deployed for a length of time necessary to allow for effective observation and assessment. This may vary in each EOM and will be determined, in large part, by the electronic voting system in place and the OSCE/ODIHR institutional experience in this context.

It may be useful for an electronic voting expert to accompany the OSCE/ODIHR Needs Assessment Mission to countries in which electronic voting is being implemented in order to identify issues that a potential observation mission should consider and to identify the documentation that may need to be requested in advance.

B. ROLE OF SHORT TERM OBSERVERS[22]

There is a need for the design of specific questions and observation tools for use by the EOM. This includes the formulation of specific questions for short term observers ("STOs"). Information collected by STOs on election day will enable the core team electronic voting expert to better assess the system.

While STOs may be unable to carry out observation of the technical aspects of the performance of any electronic voting system, there are certain aspects that are observable in the polling station on election day, including:

- Usability or user-friendliness of the electronic voting equipment, including for disabled persons, the elderly or speakers of minority languages;
- Training of polling station officials;
- Terms of delivery of equipment and conditions of storage/security of the hardware and software in the polling station;
- Who has access to voting equipment and other components of the electronic voting system in the polling station;
- Voting procedures;
- In case of observable problems, such as a voter having problems with the voting equipment or non-functioning of machines, how election officials respond to the problem; and
- Printing of a final result protocol and/or delivery of any hardware elements (memory sticks/cartridges) to higher election commissions.

Although the general task of the STO observing electronic voting should not be different

[22] Short-term Observers take part in full Election Observation Missions but not in Election Assessment Missions.

from observing regular paper voting, *i.e.,* following all the "observable" actions of polling staff and election commissions, the information that the STO should be seeking will vary depending on the system used in the particular country. In this respect, a sufficient briefing by the core team's electronic voting expert(s) in the regular STO briefing is important. The electronic voting expert(s) must inform the STOs about the main elements of the system, including the hardware used, and provide STOs with specific guidelines to help assess the performance, security, and usability of the system.

It is beneficial to include a special section on electronic voting in the STO guide as well as the STO briefing. In this manner, STOs can be provided necessary information and guidance for the observation and important information on the performance of the electronic voting system on the election day. This will help STOs assess the level of preparedness of polling station officials for the use of the equipment, as well as the level of confidence of voters and their understanding of the new procedures. Questions on the performance of the electronic voting system should be included in observation forms to be completed by STOs.

C. FUNDAMENTAL SAFEGUARDS FOR TRANSPARENCY AND PUBLIC CONFIDENCE

Fundamental safeguards for transparency should be developed for the EOM to use as a baseline for its observation of electronic voting. Participants in the OSCE Supplementary Human Dimension Meeting of 2005, which was devoted to "Challenges of Election Technologies and Procedures", agreed that "transparency and accountability of such systems are essential" and without "safeguards, audits and certification, public confidence will not be ensured".

It is a prerequisite to the use of any election system that there be broad public confidence in the system. Public confidence cannot be assumed. Indeed, in some countries, where there has existed initial public confidence in the electronic voting system, it would appear that there has been some diminishment of confidence due to either instances of system failure or public criticism of system components.

In order to assess these considerations, the following could be considered as minimal requirements for the electronic voting system in order to establish a sufficient level of transparency, accountability, and public confidence in the electronic voting system:

- Inclusive and transparent certification of the electronic voting system by a qualified independent body, under either national or international standards;
- The comprehensive testing of the system prior to its introduction and periodically thereafter;
- Access for individuals or groups specifically identified in election legislation, such as academic institutions or civil society groups, to conduct comprehensive and periodic reviews. However, such reviews should not be perceived as a substitute for the establishment of inclusive and transparent certification procedures;
- Access for international observers to the results of the certification process and domestic observer verification process;
- Secrecy of the ballot must be guaranteed;

- Security requirements and procedures that apply at each level of the system and ensure protection against external intervention, internal manipulation, and technological failure, and which ensure transparency and accountability;
- Access to documents relating to the development and implementation of standards, certification and verification of the election system;
- The electronic voting system must produce a voter verifiable paper record that the voter can view before leaving the voting booth in order to ensure that the voter's choice has been recorded accurately and to create the possibility for observers without technical expertise to observe a re-count;
- Amendment of the legal framework to take full account of the implications of new technologies, including adequate provision for access of observers, system audits and other transparency measures, as well as the possibility for recounts, mandatory audits of results, possibility for recounts, and legal challenges to election results under the new electronic voting system;
- Regulations that ensure against possible conflicts of interests of vendors, certification agencies and election officials, including a strict code of ethics to prevent the appearance of partisan activity and the acceptance of anything of monetary value between vendors and officials involved in the procurement, administration, and oversight of election systems;
- Establishment of a clear division of responsibilities between vendors, certification agencies and election administrators to fully ensure accountability and an effective response in the case of system failure.

It is questionable whether electronic voting should be introduced where there exists a significant level of distrust or dissatisfaction with the election administration. Introduction of an electronic voting system, which by its nature is more difficult to observe, may only reinforce existing distrust and further diminish public confidence in elections.

Whenever introduction of new voting technologies is being considered, it may be best to introduce an electronic voting system incrementally in order to create and maintain public confidence. The electronic voting system might be first used in some type of elections considered by voters to be less important than other types of elections. The system might be introduced in local elections before using it countrywide in national elections.

Thoughtful and careful introduction of the system to voters can greatly enhance transparency and facilitate public confidence. Incremental introduction allows voters to be educated, vendors and election administration to identify potential problems, and poll workers to become familiar with the system. Incremental introduction can also alleviate any perception that some voters might have that the system is being forced on them before it has been adequately tested and proven.

VI. CONCLUSION

The potential for increased use of electronic voting requires the development of specific guidelines for the OSCE/ODIHR to apply in its observation and assessment efforts in participating States. These guidelines should be considered in order to enhance the OSCE/ODIHR observation methodology where electronic voting is an element of a

participating State's election system. However, electronic voting is not an isolated component of an election and must be considered with other important components that are assessed by the OSCE/ODIHR.