Implementing and Overseeing
Electronic Voting and Counting Technologies

Chapter 2.2: Building the System for E–voting or E–counting

Lead Authors

Ben Goldsmith
Holly Ruthrauff

NDI NATIONAL DEMOCRATIC INSTITUTE

IFES International Foundation for Electoral Systems

This publication is made possible by the generous support of the American people through the United States Agency for International Development (USAID) under Award No. DFD-A-00-08-00350-00. The opinions expressed herein are those of the authors and do not necessarily reflect the views of USAID or the United States Government.

2.2
BUILDING THE SYSTEM FOR E-VOTING OR E-COUNTING

STANDARDS FOR IMPLEMENTATION

Once a decision is reached that a country will adopt electronic voting and counting technologies, the nation should define standards for the implementation of the system. Such national standards provide overall principles that can help to guide the development of electronic voting and counting technologies as well as the legal framework that regulates them.

The process of defining national standards for electronic and voting technologies should be as open and transparent as possible, with broad participation by recognized technical institutions and experts. Public consultation should also be part of the process, with opportunities for civil society, political actors and voters to review proposals and offer their views.

When defining national standards, countries may choose to make reference to or incorporate international standards for the use of voting and counting technologies (for example, the Council of Europe [CoE] recommendation on e-voting[28]). International standards for democratic elections defined in public international law apply equally to elections using electronic voting and counting technologies and must be taken into account. However, as explained above, international electoral standards are still evolving in order to cope with the specific challenges of using voting and counting technologies; and there is no consensus yet on their content. Even the CoE recommendation on e-voting, which is the most authoritative of the emerging standards documents, is only a recommendation and only directly applicable to CoE member states.

The CoE recommendation provides a good starting point for establishing general standards specific to electronic voting and counting technologies, both in member states of the Council of Europe, in which the recommendation has legal standing, as well as in nonmember states. Norway, for example, incorporated the CoE recommendations (with several noted exceptions[29]) in its Regulations Relating to Trial Electronic Voting, making the CoE recommendations part of the regulatory framework for the electronic voting trial. The regulations emphasize that voting should be free, direct and secret, and sets basic principles to ensure the integrity, accessibility and security of the system during the trial.

In addition to general principles for the implementation of electronic voting and counting, national standards may also include technical requirements for the systems. For instance, in Belgium, the election law includes the technical features that voting machines must comply with as well as steps for certification of equipment. Similarly, Section 301A of the Help America Vote Act (HAVA) in the United States includes technical requirements for voting machines used in federal elec-

28 Council of Europe. Recommendation of the Committee of Ministers to Member States on Legal, Operational and Technical Standards for E-voting, adopted September 30, 2004.

29 These exceptions were largely related to the requirement to certify electronic voting solutions, which the Norwegian ministry responsible for managing elections did not wish to include for the pilot process.

tions related to verifiability, audit capacity, accessibility for individuals with disabilities, alternative language accessibility, error rate and a requirement that all states adopt uniform and nondiscriminatory standards that define what constitutes a vote and what will be counted as a vote for each category of voting system.

Although not specific to e-voting or elections, there are a number of other international and national standards with which an electronic voting or counting system may need to comply. Standards on such issues as data processing, data protection, electronic transactions, usability, accessibility, security and project management are all relevant and must be taken into consideration.

It is important at the initial stages of implementation to research what standards may apply to ensure that systems are developed to be compliant. Countries may also wish to develop standards for electronic voting and counting systems by using existing private and public institutions that develop technical standards or by drawing experts from such institutions into an expert committee for this purpose.

FIGURE 10 – GUIDELINES DEVELOPMENT IN THE U.S.

Following problems with punch-card voting systems in the 2000 elections, the United States made a concerted effort to develop election standards, including standards for election equipment, that aimed to ensure a level of integrity in the country's numerous electoral jurisdictions. While this effort has been conducted in a transparent manner and has resulted in a detailed set of guidelines, it also highlights the challenges of gaining consensus on and implementing such guidelines.

The U.S. Election Assistance Commission (EAC) was established by the Help America Vote Act (HAVA) of 2002 to serve as an information clearinghouse regarding election administration; testing and certifying voting systems; and promulgating standard voting system requirements.

HAVA also established the Technical Guidelines Development Committee (TGDC), a 14-member expert board drawn from a combination of technical standards agencies and state election officials and chaired by the director of the National Institute of Standards and Technology. The purpose of the TGDC is to assist the EAC with the development of the Voluntary Voting System Guidelines (VVSG), a series of specifications and requirements that voting systems would have to meet to be certified by the EAC. The TGDC works in a transparent way, opening its meetings and archives to the public and inviting public comment and position papers on its current initiatives.

In 2005, the EAC released the VVSG for a 90-day public comment period prior to adoption of the guidelines and reviewed more than 6,000 comments. Under HAVA, adoption of the VVSG by states is voluntary, but adoption by a state brings the guidelines into force for all of the state's electoral jurisdictions.

In 2007, the TGDC prepared a set of recommendations for a revised version of the VVSG, parts of which were incorporated into a new draft proposal by the EAC. The proposed revised guidelines were released for a 120-day period of public comment in 2009, but have not yet been finally adopted.

KEY CONSIDERATIONS: STANDARDS FOR IMPLEMENTATION

FOR IMPLEMENTING BODIES

- ☑ How broad is participation by recognized technical institutions in the process for defining national standards for implementation of electronic and voting technologies?
- ☑ Has an expert committee been established to help define the national standards?
- ☑ To what extent have international/regional standards been considered in the development of national standards?
- ☑ Do the national standards consider technical features that must be complied with?
- ☑ Has consensus been achieved among experts on the defined standards?
- ☑ Have the experiences of other countries been considered in the development of national standards?

FOR OVERSIGHT ACTORS

- ☑ How transparent and inclusive is the process of defining national standards for electronic technologies? For example, are technical institutions/experts involved, and are public consultations held with civil society, political actors and voters?

- ☑ To what extent do the national standards comply with have international and regional principles, and standards, and best practices been considered in the development of national standards?
- ☑ To what extent have existing national technical requirements been taken into account?

LEGAL AND PROCEDURAL FRAMEWORK

The use of electronic voting and counting technologies should be defined in the legal framework. This process can take a considerable amount of time, particularly since key legal provisions are incorporated at the legislative level (i.e., in constitutions and electoral laws) as well as the regulatory level. Amendments should, at a minimum, address the following: physical and procedural aspects of voting or counting processes; testing and certification; audit mechanisms and conduct; status of audit records versus electronic records; transparency mechanisms; data security and retention; voter identification; and access to source code. The process of developing amendments should involve input from electoral stakeholders, including political parties and civil society.

In order to properly implement electronic voting or counting technologies, the use of these technologies needs to not only be in compliance with the constitutional and legal provisions relating to elections and the general conduct of public affairs, but must also be defined in the legal framework for elections. The legal framework includes the constitution, if there is one, the laws relating to elections, and the secondary legislation (such as regulations, rules and procedures often passed by electoral management bodies).

While constitutions rarely say anything specific about electronic voting or counting technologies, they may include general provisions that are relevant to the use of these technologies. Germany provides a good example of this (see Figure 11 below for more details), with the German Constitutional Court deciding in 2009 that the electronic voting machines used in Germany did not comply with general transparency requirements for the electoral process established in the constitution.

FIGURE 11 – THE CONSTITUTIONALITY OF ELECTRONIC VOTING IN GERMANY

After a largely successful trial period spanning from 1998 to 2005, two citizens challenged the constitutionality of electronic voting before the German Constitutional Court. Though the public generally viewed the voting system in a favorable manner throughout the trial period, the actual legality of the technology was not fully assessed in advance of implementation.

Germany piloted its first electronic voting machines, supplied by the Dutch company NEDAP, in Cologne in 1998. The trial was seen as successful, and one year later Cologne used electronic voting machines for its entire European Parliament elections. Soon other cities followed suit, and by the 2005 general election nearly 2 million German voters were using

these NEDAP machines to cast votes. Reaction to the use of these electronic voting machines was generally very positive among voters, who found the machines to be easy to use, and among election administrators, who were able to reduce the number of polling stations and staff in each polling station.

However, after the 2005 election, two voters brought a case before the German Constitutional Court after unsuccessfully raising a complaint with the Committee for the Scrutiny of Elections. The case argued that the use of electronic voting machines was unconstitutional and that it was possible to hack the voting machines, thus the results of the 2005 election could not be trusted.

The German Constitutional Court upheld the first argument, concurring that the use of the NEDAP voting machines was unconstitutional. The Court noted that, under the constitution, elections are required to be public in nature and

> that all essential steps of an election are subject to the possibility of public scrutiny unless other constitutional interests justify an exception . . . The use of voting machines which electronically record the voters' votes and electronically ascertain the election result only meets the constitutional requirements if the essential steps of the voting and of the ascertainment of the result can be examined reliably and without any specialist knowledge of the subject . . . The very wide-reaching effect of possible errors of

> the voting machines or of deliberate electoral fraud make special precautions necessary in order to safeguard the principle of the public nature of elections.[30]

Making it clear that the court's decision did not rule out the use of voting machines in principle, it stated that:

> The legislature is not prevented from using electronic voting machines in elections if the possibility of a reliable examination of correctness, which is constitutionally prescribed, is safeguarded. A complementary examination by the voter, by the electoral bodies or the general public is possible for example with electronic voting machines in which the votes are recorded in another way beside electronic storage.

This decision by the German Constitutional Court, stressing the need for transparency in the electoral process without specialist technical knowledge, effectively ended Germany's recent use of electronic voting. Although the Court decision does not rule out electronic voting machines entirely, no further moves to adopt machines that meet the transparency requirements have been made.

30 A link to the German Federal Constitutional Court's 2009 ruling can be found in the Resources section of this manual.

In addition to ensuring that suggested technology solutions are in compliance with the constitutional framework of a country, consideration should also be given to whether suggested solutions meet international standards, including emerging standards for the use of electronic voting and counting technologies. Election officials and lawmakers may wish to study other countries' experiences when considering whether to adopt such technologies.

Primary and secondary legislation will inevitably need to be amended in order to accommodate the use of electronic voting and counting technologies. It is important that key legal provisions relating to the use of electronic voting or counting system are included at a legislative level so that the use of these technologies is not entirely legislated at the regulatory level. The necessary amendments to the electoral legal framework will vary depending on the technology being implemented but should cover, at a minimum, the issues listed below:

- **Physical Aspects of the Voting or Counting Process** – The use of electronic voting or counting machines will entail changes to the procedure for the setup and conduct of voting and/or counting. For example, when direct-recording electronic voting machines are used, there is no ballot box to prepare and seal. The common practice of displaying the empty physical ballot box before polling starts does have a comparable procedure for electronic voting or counting machines; a display demonstrating that no ballots have been stored is conducted for observers at the beginning of the process. Some of the procedures relating to the setup and conduct of voting and/or counting may be in the election law(s) or may be in secondary legislation, and both will need to be reviewed and amended to accommodate the setup and use of electronic voting or counting technologies.

- **Procedural Aspects of the Voting and Counting Process** – The timeline for the preparation of the voting or counting systems should be clearly

outlined, as should details of how the system is to be operated, who is allowed access to it during elections, how equipment should be stored between elections and how access to equipment in storage should be regulated and reported.

- **Testing and Certification of Technologies** – Electronic voting and counting technologies clearly need to be tested before they are used. While any responsible election management body would ensure that sufficient testing of such technologies takes place before they are used for elections, it may be useful to guarantee that testing takes place and specify the kinds of testing to be conducted by including these requirements in the law or in secondary legislation. Likewise, if there is a process of formal certification of electronic voting and counting technologies, this should be included in the law as well. The law should also clearly identify the institutions with the authority to provide this certification, the timeframe for certification and the standards and requirements against which certification will take place.

- **Audit Mechanisms** – The need for audit mechanisms for electronic voting and counting technologies is an emerging international standard. In order to ensure that this standard is met, the requirement for an audit trail should be included in the law. The nature of the audit mechanisms may also be specified if relevant — for example, any requirement for a voter-verifiable audit trail often used with electronic voting machines.

- **Conduct of Audits** – Audits should be conducted in order to generate trust in the use of electronic voting or counting machines and to ensure that these technologies function correctly. Many different kinds of audits can be conducted, including audits of the results, audits of internal logs, audits of storage and access to devices, and so on. The law should

clearly identify which audits are to be implemented, when such audits are to take place and the scale of the audits. In addition to requiring audits, which should be provided irrespective of whether there are any electoral challenges, the law should also identify conditions under which recounts are to take place.

- **Status of Audit Records Versus Electronic Records** – In the event that the conduct of an audit determines a different result than is produced electronically by an electronic voting or counting machine, the law should specify how to deal with the situation.

- **Transparency Mechanisms** – The use of electronic voting and counting machines entails the conduct of existing electoral procedures in different ways, as well as the conduct of new stages in the electoral process (for example, the configuration of electronic voting machines). In the interest of transparency, appropriate procedures will need to be developed to ensure that political actors and observers have access to these different and new processes so that they can provide meaningful oversight of the process. These transparency measures should be clearly defined in the legal framework so that observers and party representatives understand and can utilize their access rights.

- **Data Security and Retention** – It is unlikely that existing laws and procedures adequately cover the issue of electronic data security when using electronic voting or counting machines. The way in which all electoral data is secured and stored will need to be provided for in the legal framework, as will the timeframe and procedures for deletion of the electronic data, and these provisions must be in accordance with existing data protection legislation.

- **Voter Identification** – If identification/authentication is being incorporated into the electronic voting process, then this may require legislation, whether using biometrics or making mandatory a particular form of machine-readable ID. In such cases it is essential that the secrecy of the vote be protected through de-linking the vote and the identity of the voter.

- **Access to Source Code** – It may be prudent to legislate whether source code is open source or not, in addition to legislating the mechanisms for any access by stakeholders.

Many of these issues are covered in greater detail later in this part of the guide, and the intention here is to identify the issues that are relevant for inclusion in order to properly legislate for the use of electronic voting or counting technologies.

It is clear from the preceding discussion that adapting the legal framework for the use of electronic voting or counting technologies will entail considerable amendments to laws and secondary legislation. Electoral stakeholders must be involved in the development of these legislative and regulatory amendments. Initially, political parties and observers should be consulted on the ways in which the legislation needs to be changed, especially from a transparency and oversight perspective. Once legislation is passed, the election management body will need to fully brief political parties, the media and civil society on the changes that have been made.

KEY CONSIDERATIONS: LEGAL AND PROCEDURAL FRAMEWORK

FOR IMPLEMENTING BODIES

- ☑ Are the electronic voting and counting technologies in compliance with the constitution and/or electoral legislation?
- ☑ Are suggested electronic voting and counting technology solutions in line with international and emerging standards?
- ☑ Is the timeline for preparation of voting and counting systems clearly outlined in the legal framework?
- ☑ Are requirements included for the testing of voting and counting technologies prior to their use in the elections?
- ☑ Is an audit trail legally mandated, and if so, is the nature of the audit mechanism specified and is the type of audit, timeframe and scale of audit clearly identified?
- ☑ Have conditions under which audits and recounts are to take place been identified?
- ☑ Are there specifications for dealing with a situation in which the audit produces a different result than by an electronic voting or counting machine?
- ☑ Does the legal framework include specifications for how electoral data will be stored, and the timeframe and procedures for deletion of electronic data in accordance with existing data protection legislation?

- ☑ Does the legislation address identification/authentication issues if they are being incorporated into the electronic voting process?

FOR OVERSIGHT ACTORS

- ☑ Are the electronic voting and counting technologies in compliance with the constitution and/or electoral legislation? Are they in line with international and emerging standards?
- ☑ Is the appropriate secondary legislation in place to accommodate the implementation of electronic voting and counting and the processes associated with such technologies?
- ☑ Are transparency mechanisms included and clearly defined in the legal framework, such that oversight actors have sufficient access to the new processes associated with the technologies?
- ☑ During the electoral legal framework reform process, has the election management and/or legislative committee consulted political parties and civil society on the ways in which the legislation needs to be changed?
- ☑ After the legal framework has been revised , have parties and civil society been briefed on the reforms enacted pertaining to election technologies?

DESIGN REQUIREMENTS

By defining general requirements on the design of the electronic voting or counting system, electoral authorities provide an indication to potential suppliers of what their overall needs are. System design should ensure transparency, accountability, secrecy, usability, accessibility and security. Design requirements should ideally be informed by testing of equipment on different groups of voters. The design process should involve the input of relevant stakeholders, such as parties and civil society. The design process should also consider and specify any additional components (beyond electronic voting and counting equipment) that must be provided as part of an overall election management system.

The starting point for the development of an electronic voting or counting system is for the election administration body to define a set of general requirements that a system should meet. These general requirements should be in line with any national or international standards (including emerging electronic voting standards), as well as the country's own legal framework.

General requirements should provide broad guidance on the design of the electronic voting or counting system. They should address issues such as secrecy, transparency, accountability, usability/accessibility and security. For instance, such requirements might indicate what kind of audit trail is necessary or whether source code must be open or verifiable.

The process of defining design requirements should be an inclusive one, seeking the input of various stakeholders, including political parties and civil society. Such consultation will help to ensure broad support for the system that is eventually selected, as well as provide specific information on the needs of particular target groups.

By defining general requirements, election authorities give potential suppliers of voting and counting equipment an indication of what their overall needs are. Once these requirements are agreed on, authorities can review different options offered by vendors to determine whether any already developed off-the-shelf products meet the requirements or whether a new system will need to be designed.

Of particular importance are design requirements regarding the usability and accessibility of the electronic voting or counting system. The system should be as user-friendly as possible to maximize the ability of all voters to cast their ballots in an accurate, effective and efficient manner. At the same time, electronic voting and counting systems should be designed to maximize opportunities for the inclusion of voters who may normally struggle to participate in the electoral process, such as voters with visual impairments, hearing impairments or motor difficulties, as well as those from minority language groups. New technologies can increase the ease of access for such groups, and election authorities should make requirements for such accessibility explicit in their initial design requirements.

The UN Convention on the Rights of Persons with Disabilities sets the overall norm for ensuring that persons with disabilities have equal access to the same services as the rest of the population. Article 29 of the convention explicitly requires state parties to ensure that persons with disabilities can participate in political and public life on an equal basis with others; this includes the right and opportunity to vote. It further requires that appropriate procedures, facilities and materials be provided that are accessible for persons with disabilities and that protect their right to cast secret ballots. The Council of Europe Recommendation on Legal, Operational and Technical Standards for E-voting also addresses accessibility, suggesting that e-voting systems should maximize opportunities for people with disabilities.

A number of standards relating to usability and accessibility are not tied specifically to voting, but instead seek to make technology as accessible as possible, and are therefore directly relevant to the design of electronic voting and counting equipment. For instance, the International Standards Organization (ISO) has developed standards on the interaction between humans and machines that do not specifically relate to electronic voting and counting, but that can be usefully adopted to maximize the accessibility of such systems. Similarly, the Web Accessibility Initiative (WAI) has developed operational guidelines to ensure that persons with disabilities have the best possible access to content on the web. WAI guidelines are particularly relevant for Internet voting.

Election authorities can incorporate standards related to usability and accessibility into their design requirements to ensure that voting and counting systems are developed in a manner that maximizes usability for all voters as well as the access afforded to particular groups of voters. For instance, in Norway, election authorities referenced specific accessibility and usability requirements as part of their tender for electronic voting solutions. This reflected the emphasis Norway put on making elections as inclusive as possible.

The usability and accessibility of a particular voting or counting system can best be assessed through the testing of equipment on different groups of voters throughout the design phase. Such testing should be as inclusive as possible, involving voters from different demographics as well as those who might normally struggle to participate. Election authorities should liaise closely with NGOs that represent particular groups such as persons with disabilities, minority language communities and illiterate or low-literacy voters to understand their needs in the voting process and to maintain an ongoing dialogue about the development and testing of the equipment.

Testing of electronic voting and counting options with voters also provides an opportunity to enhance the transparency of the development process and boost public confidence in the system. Involving political actors and citizen ob-

server groups in the development testing process should also help to promote transparency and confidence in the resulting system.

If election authorities determine that off-the-shelf solutions are not available that meet the general requirements, it is likely that customized equipment will need to be developed. In such cases, technical experts will need to develop the specific technical requirements for the equipment. It is important that throughout the development process, details of the work of such experts is made available to the public. Such experts should be independent from state authorities and political contestants, and should disclose any affiliations with interested parties so as to avoid any perceived or real conflicts of interest where particular vendors could be seen to receive preferential treatment.

Additional factors for practical use and storage of the equipment should also be considered in the design phase, such as: whether there are particular environmental conditions in which the equipment will be required to function (e.g., high temperatures, humidity or dust); whether the power supply is uncertain in some parts of the country; how equipment should be transported and whether this is an issue for the design; and the environmental requirements that should exist for storing the equipment between elections.

For Bhutan's 2008 parliamentary elections, election authorities decided to use the lightweight (5 kilogram) battery-powered electronic voting machine used in India, as the machines needed to be transported by officials to distant villages, sometimes on foot.[31] Consideration of such factors early in the design phase is absolutely crucial for the successful implementation of electronic voting and counting equipment.

It should also be noted that it is not only the design of voting or counting machines themselves that needs to be considered and specified. An electronic voting or counting system may be part of an overall election management sys-

31 Election Commission of Bhutan, "Electronic Voting Machines," www.election-bhutan.org.bt.

tem. This election management system may be used to manage the administrative aspects of the election related to the machines (for example the pre-election configuration) and also to integrate candidate registration and verification with ballot production, issue of election notices, production of polling cards, count tabulation and results publication. If any or all of these components are required to be provided as part of an overall election management system, then they will need to be specified in advance.

FIGURE 12 – DESIGN AND PROCUREMENT OF E-VOTING MACHINES IN BRAZIL

The design and procurement processes carried out in Brazil demonstrate the importance of transparency and inclusiveness in building trust not only in the design and procurement of technology, but also in the eventual technology itself.

In 1994, Brazil's Tribunal Superior Eleitoral (TSE) established a committee to assess the feasibility of transitioning to electronic voting. While the committee was largely made up of legal professionals, it reached out to a wide range of stakeholders through the consideration and design stages of its work. Stakeholders within government were consulted, but so were outside experts at a range of computer companies. Existing commercial electronic voting packages were also assessed, and a visit was conducted to the U.S. state of Virginia to see the electronic voting machines in use there.

The committee's conclusion from this consultation and research process was that no existing electronic voting systems met the specific requirements of Brazil's elections; therefore, a custom solution would have to be developed. In its 1995 report, the committee elaborated a set of initial requirements that would need to be met by the new electronic voting system .

The recommendations of this report led to the establishment of a "technical" committee tasked with further defining the requirements of the new system and outlining the procurement process and the evaluation of bids. In order to develop the request for tender, the technical committee first published a request for comments and suggestions. Dozens of reports from companies, government entities and universities were received in response to this request; and with the information received, the technical committee wrote detailed tender documents. The procurement process included a requirement that all bids include a working model of the proposed voting machine that could pass 96 separate tests before being considered. Five companies submitted bids initially, but only three of these provided working models that passed all 96 tests. Procurement rules for government purchases were followed, and all criteria for judging bids by companies were made public.

This open and consultative design and procurement process did much to generate trust in the process and the eventual use of electronic voting machines in Brazil.

KEY CONSIDERATIONS: DESIGN REQUIREMENTS

FOR IMPLEMENTING BODIES

- ☑ Do the general requirements set out for an electronic voting and/or counting system address issues of secrecy, transparency, accountability, usability/accessibility and security?
- ☑ Is there a process to ensure consultation and solicit feedback on the general requirements for an electronic voting or counting system?
- ☑ Do existing products meet the requirements or will a new system need to be designed?
- ☑ Does the system maximize the ability for all voters to cast their ballots in an accurate, effective and efficient manner?
- ☑ Does the system meet existing standards on usability and accessibility?
- ☑ Are external factors such as the environmental conditions in which the equipment will be required to function and the reliability of the power supply throughout the country been considered for the design requirements?
- ☑ How will equipment be transported and stored and do these considerations impact the design of the equipment?

FOR OVERSIGHT ACTORS

- ☑ Is the process of defining design requirements inclusive by, for example, seeking the input of various stakeholders, including political parties and civil society?
- ☑ Are there specific requirements to ensure that the systems are developed in a manner that maximizes the usability for all voters and the access afforded to groups of voters who may normally struggle to participate in the electoral process, such as voters with visual impairments, hearing impairments or motor difficulties, as well as illiterates or those from minority language groups?
- ☑ What tests and/or research, if any, have been conducted to assess the usability and accessibility of equipment? Was it conducted among voters from diverse demographics and among those who may normally struggle to participate?
- ☑ Is the work of developing technical requirements made available to the public?
- ☑ Are the experts responsible for developing design requirements mandated, and are they required to disclose any affiliations with interested parties (i.e., potential vendors)?

PROCUREMENT, PRODUCTION AND DELIVERY

The procurement and production processes are vitally important to building trust in the process. The procurement specification should cover everything that is required from the technology provider. It is especially important that the procurement of such technologies is conducted in an impartial manner through a transparent, competitive bidding process. Conducting such a process takes a significant amount of time and involves several different steps, as detailed below. The evaluation of bids should provide sufficient written documentation so that observers can learn whether the decisions were made strictly on the basis of the evaluation criteria laid out in the procurement documents. Contractual documents should be made available to stakeholders to the extent the law allows. Observers should use these contractual documents as tools to monitor the extent to which vendors meet their obligations. Because there is a need for frequent communication between supplier and election management body to ensure that the technology solution delivered meets the exact needs of the users, sufficient time for this interaction should be factored into the production and delivery timeline.

Once the decision to conduct a pilot or to implement electronic voting or counting technologies more generally has been made, a critical first step is procuring the equipment needed to implement the technology. A comprehensive specification is essential for this procurement process. Ideally a specification will have been developed during the decision-in-principle process and refined during the pilot, if there was one. Regardless, it is crucially important to ensure that a specification is developed that covers everything that is required from the technology provider.

A comprehensive specification should include the following issues:

- **Type of Technology** – The specification should indicate whether the election management body is interested in electronic voting, electronic counting, remote voting or a combination of these.

- **Scale** – The quantity of any equipment or services required may influence the ability of the supplier to deliver these items on time and therefore should be clearly specified, especially if custom-made equipment and software need to be developed. The anticipated number of voters using a system will also impact the suitability of systems and will be highly relevant for solutions such as remote voting systems.

- **Timeframe** – The timeframe for delivery will also have a significant influence on suppliers' ability to deliver and, potentially, on the cost of equipment and services as well.

- **Voter Authentication** – Any requirements for voting machines to also authenticate the identity of voters should be clearly identified, as should the mechanisms that will be used to conduct this authentication, such as biometric fingerprint identification.

- **Audit Mechanisms** – Any requirements for audit mechanisms should be clearly outlined.

- **Results Transmission Mechanisms** – The means by which results are to be transmitted or transferred from individual voting or counting machines to the central vote tabulation system should be defined.

- **Power and Environmental Conditions** – Any requirements for machines to operate for periods of time without mains power or to function in extreme temperatures, humidity or dusty conditions should be identified.

- **Electoral Systems** – The electoral systems that the electronic voting or counting equipment are to be used for should be identified. It may also be prudent to ensure that the equipment is able to cope with other electoral systems that are not currently used but might be adopted in the future. The specification should also indicate if each voter will need to cast multiple ballots and whether different electoral systems will apply to different ballots.

- **Accessibility Requirements** – Any requirement for the equipment to deal with multiple languages and voters with disabilities should be detailed, including the need for visual, audible and tactile interfaces, as applicable.

- **Security Requirements –** Security requirements for the electronic voting or counting machines, as well as any security standards that they should comply with, should be detailed.

- **Access to Source Code –** It is seen as increasingly important that electronic voting and counting solution source code be open to external inspection, if not fully open source, and any such requirements should be included in the specification.

- **Additional Services** – Other required services, such as project management, configuration, training and support during implementation of the electronic voting or counting technology, should be identified.

- **Consumables** – The specification should indicate whether it is acceptable for consumables, including paper, ink, cutters, batteries, memory storage units and devices, to be proprietary or whether they must be generic. If only supplier consumables can be used, will the supplier guarantee availability throughout the lifespan of the device, which might be as long as 15 years?

- **Additional Software Systems** – There may also be a requirement to procure a results transmission, receipt and tabulation system or a more general election management system that would include the electronic voting or counting system.

Comprehensive specifications will form the basis for the procurement of electronic voting or counting equipment.

While not part of the specification of requirements for electronic voting or counting technologies, the request for proposals issued with the specification may also seek information on a range of other issues relevant to the suitability of the proposals made by suppliers. These include:

- The institution that will own the intellectual property rights for the procured electronic voting or counting solution (for example, the EMB or the supplier)

- Responsibility for the repair of faulty or damaged equipment (whether it lies with the EMB or the vendor) and whether the EMB is authorized to make any repairs

- Mechanisms for configuration of electronic voting or counting machines prior to each election

- The vendor's responsibilities regarding transferring skills and knowledge to the EMB for training its staff and staff operation of the technologies

- Consequences for the integrity of stored or in-process data transactions in the instance of a sudden loss of power to equipment

- Maximum capacity of electronic voting or counting machines in terms of the number of electoral races and candidates that can be accommodated

- Means of verifying that loaded software is the approved version

- Mechanisms to demonstrate that the electronic version of the ballot box is empty at the beginning of voting and/or counting

- Capacity of the electronic voting system to display photographs or symbols for ballot entities

- Mechanisms for review and confirmation of voter choices on the electronic voting solution

- Specifications and reliability of any printing device attached to the voting machine

- Mechanisms for ensuring the protection of data and secrecy of voters' choices

- Mechanism for generation of results at the end of voting or counting, and the ways in which these results are transferred or transmitted for tabulation

- Details of the election management system used with the electronic voting or counting technology, including whether the supplier is responsible for providing the tabulation system (software and hardware)

- Responsibilities and capacities for troubleshooting and other servicing before and during Election Day processes

- Life expectancy of electronic voting or counting equipment

- Maintenance and storage requirements for equipment between elections

Given that the use of electronic voting and counting technologies presents particular challenges to the transparency of and trust in the electoral process, it is especially important that the procurement of such technologies is conducted in an impartial manner, ideally using an open and transparent competitive bidding process. The conduct of an open and impartial procurement process takes time and may involve many different steps and accommodations, including:

- Consultations with technical experts during the preparation of specifications

- Establishment of eligibility requirements for bidders

- Submission of expressions of interest by suppliers

- Evaluation and prequalification of suppliers based on the expressions of interest

- Publication of the final request for proposals (RFP)
- Conduct of a vendor conference to answer questions concerning the RFP
- Time allocation for drafting and submission of proposals
- Evaluation of proposals
- Submission and responses to clarifying questions on proposals
- Publication of the selection decision
- Time for contracting the selected supplier

As can be seen from this long list, the procurement process can be lengthy, and election management bodies need to plan accordingly.

Often a committee is established to review proposals received by suppliers; the committee then evaluates the bids according to the criteria established and decides on which proposal best meets the needs of the election management body. The criteria that will be used for evaluation should be defined before the procurement process and, ideally, communicated in the RFP. Evaluation criteria might include compliance with technical specifications, experience in delivering similar solutions, quality and experience of the project management team offered by the vendor, access provided to source code and cost of the proposed solution.

The work of this evaluation committee should be transparent, and the committee should provide sufficient written documentation so that observers can learn whether the decisions were made strictly on the basis of the evaluation criteria laid out in the procurement documents. Opening the evaluation process to observers would further help to promote transparency.

Even after selection of a vendor, there should be sufficient time allocated for reaching agreement on a contract. Many vendors have their own contract templates, as do many procuring entities. Discrepancies often arise as to the specific details, such as where the equipment will be delivered (to the airport or to the warehouses of the EMB, for example), the schedule of payments, the schedule of deliveries, factory acceptance test plan, the court system that will have final jurisdiction in case of legal dispute, any exemption from taxes or the party responsible for any taxes, and whether the equipment can be used for other purposes besides the conduct of elections.

The contract should include a timeframe for the delivery of equipment and services. The election management body will need to carefully monitor the progress of the supplier in meeting its contractual obligations and must have in place contingencies for the possibility that the supplier does not deliver on time. The election management body may consider including penalties in the contract for late delivery of equipment and services to protect itself against costs associated with late delivery and provide incentives for the supplier to meet its delivery obligations.

To the extent possible under existing administrative statutes or legal mandates, contractual documents should be made available to stakeholders. In this way, observers can evaluate the contractual terms and assess, for example, whether the timeline is realistic and what the obligations of vendors are if the timeline or other terms are not met. Observers can then also monitor the extent to which vendors comply with their obligations during the process.

It should also be noted that considerable communication will likely be required between the supplier and the election management body as electronic voting or counting equipment is developed, in order to clarify and add detail to the specifications used in the procurement process. This will especially be the case where a custom-made solution, rather than an off-the-shelf solution, is

delivered. This interaction between supplier and election management body is essential in ensuring that the technology solution delivered meets the exact needs of the users, and adequate time for this interaction should be included in the timeline for production and delivery.

KEY CONSIDERATIONS: PROCUREMENT, PRODUCTION AND DELIVERY

FOR IMPLEMENTING BODIES

- ☑ Do the procurement documents for e-voting or e-counting hardware include technical specifications that detail key issues required of vendors including types of technology, security and authentication mechanisms, environmental conditions, accessibility requirements, software and source code requirements?
- ☑ Does the Request for Proposals outline expectations regarding intellectual property rights agreements; division of responsibilities between vendor and EMB; specifics of electoral system that equipment has to address; specifics for security of voting or counting equipment; hardware and software requirements for results production and dissemination systems; and maintenance and storage requirements.
- ☑ Is the evaluation criteria detailed in the Request for Proposals?
- ☑ Does the procurement process put in place mechanisms to ensure that all steps of the process are transparent and engage electoral stakeholders at appropriate steps in the process?
- ☑ Is sufficient time allocated for the procurement process to meet transparency and inclusiveness goals?

- ☑ Is there sufficient time allocated for the EMB to come to terms on a contract with the selected vendor?
- ☑ Does the contract vehicle contain specific benchmarks for timely delivery of equipment and services from the selected vendor, as well as clearly defined penalties for failure to meet benchmarks?
- ☑ Are contractual agreements made publicly available?

FOR OVERSIGHT ACTORS

- ☑ Do the procurement documents cover everything that is required from the technology provider (see above)?
- ☑ Is the overall procurement process conducted in an impartial and transparent manner?
- ☑ Is the bidding process open to all vendors and competitive?
- ☑ Are the criteria for evaluation defined before the procurement process and communicated in the bidding document?
- ☑ Is the evaluation process transparent, and does it provide sufficient written documentation that allows observers to determine whether decisions were made strictly on the basis of the evaluation criteria?
- ☑ Does the selected vendor have any links to and/or conflicts of interest with relevant public officials, political leaders, candidates and/or parties?
- ☑ Are contractual documents made available to the public, so that observers can monitor the extent to which vendors comply with their obligations during the process?

- ☑ Does the contractual arrangement ensure that the EMB will remain in control of the relationship with the vendor and that the vendor is accountable to the EMB? Similarly, is the role of the vendor vis-à-vis the EMB clearly defined?

- ☑ Is the contractual timeline realistic? What are the obligations of vendors if the timeline or other terms are not met?

SECURITY MECHANISMS

The security of electronic voting and counting systems is essential to ensuring public confidence and overall electoral integrity. At the same time, these technologies present a host of security challenges, including physical security of equipment, openness to review of the source code, secrecy of voting data, encryption of data stored on machines and transmitted to tabulation centers and verification of the legitimacy of the sources of data transmitted to tabulation centers. Because numerous security flaws have been detected in voting and counting machines in many countries, public debate on and scrutiny of the security of such technologies has increased. EMBs too often assume that systems are secure, while other electoral stakeholders often have greater distrust in technologies. Thus, EMBs need to take security concerns extremely seriously.

System security is a crucial feature of electronic voting and counting technologies. These technologies are inherently less transparent than the use of paper ballots, where all steps of the voting and counting process are observable. If an electronic voting or counting system is to be trusted by electoral stakeholders, it is important that the security challenges presented by the use of the technologies are understood and addressed.

Many aspects of this issue of system and data security need to be considered.

One key concern is the openness to review of the source code for the electronic voting or counting machine, as well as any other software related to the machines. Whether the source code for electronic voting and counting applications should be open source (i.e., published for anyone to inspect) is a significant issue in the debate about the transparency and security of these technologies.

Traditionally the source code for these machines and supporting applications has been seen as proprietary in nature, exclusively owned by the supplier and not provided for any independent review. Proprietary source code carries two inherent risks for the EMB: that it may be locked into a long-term agreement with the solution provider; and/or that future supplemental procurement of new machines may not be compatible with the ballot or results format of the existing systems. The need for transparency in the electoral process has led to increasing demands from election management bodies for this source code to be open to inspection by external stakeholders, and increasingly, suppliers are meeting these demands.

This issue is relevant for security, in that the source code for voting and counting applications is often very long and complex. Errors and omissions, whether accidental or otherwise, may exist in the software and not be found, despite internal review. Allowing external stakeholders to inspect the code should dissuade the inclusion of deliberately malicious code by suppliers or rogue programmers. It is also expected that the more people that can check the source code, the more likely it is that errors in the code can be identified and corrected. Given the complexity of source code, political party observers and nonpartisan election observer groups will likely need to engage IT security experts to review the code and other aspects of the security mechanisms.

Maintaining secrecy of the voting data, including ensuring that votes are not linked to voters' identification information, is a particular security challenge for

electronic voting and counting machines, especially with remote voting, where identification details need to be entered into the same device on which the vote is cast (for example, a personal computer). However, this is increasingly an issue with electronic voting machines used in supervised environments, as voting machines are now being developed to identify each voter through a personal ID number or through biometrics.

FIGURE 13 - THE IMPORTANT USES OF CRYPTOGRAPHY IN ELECTRONIC VOTING AND COUNTING

Cryptography offers a number of benefits to electronic voting and counting solutions. It may be used to perform tasks such as encrypting votes and digital ballot boxes, ensuring votes and software are unmodified, verifying the identity of a voter before he or she casts a ballot, and assisting in auditing and tallying the results of an election. Traditionally, cryptography (from the Greek for "hidden writing") was used to conceal information between two people using a secret key known only to them. Over time, it expanded into the art and science of using mathematics (in the form of algorithms) to hide information, protect privacy, ensure files are not altered and prove the identity of a message's sender. Considering the paramount importance of ballot secrecy and fraud detection, cryptography has proved a useful tool for countries employing election technologies.

ENCRYPTION AND DECRYPTION

Encryption and decryption are among the most common uses of cryptography. Encryption is the process of obscuring information, and decryption reverses this process. Keys are the secret piece of information necessary to encrypt and decrypt data. Encrypted data is unintelligible; and without the correct decryption key, it cannot be recreated in its original form. An example of a very simple encryption key is to increment each letter in a block of text by one letter (i.e., "a" becomes "b," "b" becomes "c," etc.), so "Election Day" would become "Fmfdujpo Ebz". Decryption of the text requires that each letter be decremented by one.

Ensuring that a key remains secret is paramount to ensuring encrypted information remains hidden. With the advent of computer-based cryptography, keys are now represented as large, nearly random strings of letters and numbers such as 2b7e151628aed2a6abf7158809cf4f3c (this number would typically be much larger). Different methods of encryption and decryption have different properties; some function more quickly, are more difficult to break, can be transmitted more rapidly or work better on slower computer processors.

For electoral purposes, encryption is often used to obscure the contents of a voter's ballot selections and the contents of a digital ballot box. The voter's encrypted ballot selections may be stored on a voting machine or sent over an insecure channel like the Internet or the telephone network. When casting an electronic vote, the value of the vote will be encrypted

using an encryption key produced by the EMB and available at all electronic voting locations. However, only the EMB will have the key that is needed to decrypt encrypted data.

HASH FUNCTIONS

Another cryptographic function is the hash (often called cryptographic hashes). Hashes are mathematical functions or equations that "read in" a piece of information (e.g., a file) and output a set of numbers and letters that are unique to the input. Just as with encryption, there are different hashing algorithms with unique characteristics. Using the SHA-256 hashing algorithm, the word "election" hashes to: c7a19845b9e9de079260094d79525957. But when using the same algorithm and inputting the word "elections" (notice there is only a one-letter difference), the output is completely different: b9dd4e28c0fe5673909bb6c0615f5f22. This is the point of hashes – detecting changes. A file of any size can be passed through the hashing algorithm, even large and complex computer programs. Hashes can identify a one-character modification to a vote stored on a computer, the software running on a voting machine, or even an entire operating system.

There are many applications of this concept to voting. In the U.S., a public repository known as the National Software Reference Library (NSRL) stores the hashes of voting system source code and the compiled versions of software that are used for voting and counting systems. Some EMBs verify all software before installing it on voting machines

by "hashing" the software and checking the result against the hash values in the NSRL. This process helps to identify malicious modifications to the software, but many election officials also state this process helps identify when incorrect versions are about to be installed or when software is corrupted.

DIGITAL SIGNATURES

Digital signatures are mathematical functions that work in a similar manner to cryptographic hashes and also help identify who sent a message or file. Digital signatures are not analogous to physical handwritten signatures as they provide much stronger proof of who "signed" a message. A digital signature is different for every message, making it much more difficult to forge another person's signature. In elections, digital signatures are used to "sign" the contents of a digital ballot box or a voter's ballot selections, thus helping ensure the ballot box or vote was not altered. If tampering occurred and the digital signature was forged, the attacker would need to know another person's, or the EMB's, secret key.

MIX-NETS

The order in which data is stored on electronic voting or counting systems can be used to link the identity of the voter to the value of the vote, if the order in which voters cast their ballots is also observed. Cryptographic schemes have been developed to protect the secrecy of stored votes. A mix-net takes encrypted, stored data and then re-encrypts it and mixes the order in which it is stored. Only then are the data

decrypted and the values of the votes revealed. As the order of the original vote data has been changed and the encrypted value of the stored vote data has also been changed (it was re-encrypted as it passed through the mix-net), there is no way that decrypted vote values can be linked back to either the original data received or the identity of voters.

HOMOMORPHIC CRYPTOGRAPHY

Another solution used to protect the secrecy of stored votes is homomorphic cryptography, which allows the votes in the electronic ballot box to be tabulated while still encrypted. As individual votes are never decrypted, there is no possibility of linking voters to the way that they voted. Votes may even be posted to a public bulletin board for independent tabulation by anyone to verify the outcome of the election.

The physical security of electronic voting or counting machines and the data held on the machines also needs to be protected. Access to voting or counting machines must be controlled, and any access that takes place should be recorded, reported on if it is outside of standard operating procedures and, ideally, conducted by two-person teams. Data ports on electronic voting or counting machines may be essential so that software and configuration data can be loaded onto the machines, but the data ports need to be protected so they cannot be used to manipulate the functioning of the machines or to insert different vote data. It is also important that mechanisms are in place to verify that the software loaded onto any electronic voting or counting machine is the same version that was tested and approved by the election management body and external stakeholders.

Data held on electronic voting or counting machines needs to be encrypted to ensure that, even if the data is accessed by unauthorized persons, this data cannot be read, used or manipulated. Procedures must also be in place to ensure the security of decryption keys and to establish when and how the decryption of data takes place.

The encryption of voting data needs to be maintained when it is transmitted or transported from individual electronic voting or counting machines to the tabulation system for generation of results. There also must be a way to ensure that data uploaded to the results tabulation system has come from a legitimate source. This can be achieved by digitally signing data and only allowing data with an authorized digital signature to be uploaded.

In the public debate about electronic voting and counting systems, their security has become an increasingly important issue, with systems subject to considerable scrutiny. Electronic voting and counting machines and results systems have not fared well under this additional scrutiny. Despite the denial of suppliers (and often of election administrators as well), numerous security flaws have been detected in voting and counting machines. In the Netherlands campaigners argued that it was easy to reprogram voting machines to, for example, play chess or to manipulate the election results. When the suppliers of the machines challenged this, the campaigners reprogrammed one of the voting machines to do exactly that, playing chess against a reprogrammed voting machine (see Figure 14 below for more details).[32]

In India, the election commission claimed that, because the instructions for their voting machine were burned into the circuit board, it was not possible to reprogram their machines. Rop Gonggrijp, a Dutch hacker who was involved in exposing the vulnerability of the Dutch voting machines, along with a number

32 Gonggrijp, R. and Hengeveld, W-J (2006) "Nedap/Groenendaal ES3B Voting Computer: A Security Analysis."

of other researchers, took on the challenge of showing whether the Indian voting machines were secure. They demonstrated that, with little effort, the Indian voting machines could be manipulated to change the results, avoiding this circuitry coding, and that this manipulation could even be activated remotely by mobile phone.[33]

In the U.S., the debate on electronic voting machine security has been particularly intense, with many studies demonstrating how existing voting and counting machines could be hacked in order to manipulate election results. In 2004 the source code for a commonly used electronic voting machine in the U.S. was published online. A group of four computer scientists set about analyzing the source code and discovered several problems, including the incorrect use of cryptography, vulnerabilities to network threats and poor software development processes. This analysis concluded that the voting machine system was vulnerable to both inside and external security threats and failed to meet even minimal security standards.[34]

Concerns about the physical security of the Irish voting machine were also identified by that country's Commission on Electronic Voting. In its first report in 2004 on the electronic voting system chosen in Ireland, after an initial small pilot of the voting machines in 2002, the commission found security defects in both the hardware/software interface and the physical voting machine itself.[35] The system did not use (then) current security mechanisms, such as cryptography, and was vulnerable to attack by an insider with short-term access to the machine, with the result that recorded votes could be significantly affected. The commission raised serious concerns about the integrity of any elections held

33 Prasad, H. K., Haldermann, J. A., Gonggrijp, R. Wolchok, S., Wustrow, E., Kankipati, A., Sakhamuri, S. K. and Yagati, V. (2010) "Security Analysis of India's Electronic Voting Machines."

34 Kohno, T., Stubblefield, A., Rubin, A. and Wallach, D. (2004) "Analysis of an Electronic Voting System," IEEE Symposium on Security and Privacy. (Washington, DC: IEEE Computer Society Press) avirubin.com/vote.pdf.

35 Commission on Electronic Voting (2004) "First Report of the Commission on Electronic Voting on the Security, Accuracy and Testing of Chosen Electronic Voting System," Appendix 2B.

using the machines and determined that they should not be used again before further efforts were made to resolve these issues.

The experiences of these countries has led to a tendency to put any electronic voting or counting system under intense scrutiny. All too often election management bodies seem to operate under the assumption that electronic voting and counting systems are secure until proven otherwise. At the same time, electoral stakeholders tend to start from a position of much greater distrust in such technologies. In this context, election management bodies need to take security concerns very seriously and must be seen to address both real and perceived security threats.

FIGURE 14 – THE NGO CAMPAIGN ON THE SECURITY OF E-VOTING MACHINES IN THE NETHERLANDS

The Netherlands' experience provides an example of the challenges that can arise when EMBs, political parties, civil society and other stakeholders do not pay adequate attention to the integrity and security of electronic voting and counting technologies.

In the summer of 2006, a number of computer experts in the Netherlands launched a group called "We Do Not Trust Voting Computers" ("Wij vertrouwen stemcomputers niet") to publicize their concerns about the security of electronic voting machines and their lack of auditability mechanisms. The

use of electronic voting machines was already widespread in the Netherlands, although Amsterdam introduced them for the first time during municipal elections in spring 2006.

The campaign set up a website (http://wijvertrouwenstem-computersniet.nl) and sought to further investigate the use of electronic voting computers through freedom of information requests. The requested documents revealed a number of security flaws in the voting machines, as well as the extent to which the election process had been outsourced to technology suppliers. The campaign posted the documents on its website, generating controversy with the technology suppliers who claimed the documents included confidential information. The controversy brought increased media attention to the campaign.

The campaign received widespread national exposure in early October 2006 when its experts appeared in an investigative television news program demonstrating the security flaws of the voting machines. The program showed the experts replacing the memory chip in a voting machine in less than five minutes, allowing them to manipulate the results of a mock election; later they reprogrammed the machine to play chess. The report also raised serious questions about the physical security of the machines while in storage and during transport, the testing of machines and the adequacy of the regulatory framework. The campaign released a security analysis at the same time detailing the vulnerabilities identified by

the experts, including the possible detection of radio emissions outside polling stations that could compromise the secrecy of the vote.

Following government testing of the machines and an independent review of the election process (see Figure 26, "Re-evaluation of the Use of Electronic Voting Machines in the Netherlands" below), the Dutch Parliament withdrew the enabling legislation for electronic voting in October 2007, returning the country to nationwide paper balloting for the first time in over 40 years.

KEY CONSIDERATIONS: SECURITY MECHANISMS

FOR IMPLEMENTING BODIES

- ☑ Have the advantages and disadvantages of open source code versus proprietary code been fully considered in the design process?
- ☑ Is a mechanism in place to control access to voting or counting machines? Does the control mechanism include recording and reporting of access to the machines that is outside of standard operating procedures?
- ☑ Is the data held on electronic voting or counting machines protected through encryption?

- ☑ Are procedures in place to ensure the security of decryption keys and to establish when and how the decryption of data takes place?
- ☑ Is the encryption of voting data maintained when it is transmitted or transported from individual electronic voting or counting machines to the tabulation system for generation of results?

FOR OVERSIGHT ACTORS

- ☑ Does the system only allow access for authorized users, and is that access provided in a secure manner?
- ☑ Is the physical security of machines, including data ports, protected from would-be attempts to manipulate the machines? Are party agents and election observers able to monitor any intervention that affects the system while voting and counting being conducted?
- ☑ Is the secrecy of the vote maintained, such that votes are not linked to voter identification information?
- ☑ Are there mechanisms, such as hashes, to ensure the software loaded onto machines can be verified as the EMB-tested and approved version?
- ☑ Is voting data encrypted to ensure it can be securely transmitted or transported from individual machines to the tabulation system? Is there a mechanism, such as a digital signature, to ensure that data transmitted to the tabulation system is from a legitimate source?

RECRUITMENT AND TRAINING OF PERSONNEL

One of the most difficult challenges for EMBs in transitioning to electronic voting and counting technologies is building the capacity at all levels to administer elections with new technologies. This usually involves not only training existing staff, but also creating new structures and hiring new staff with the skills necessary to oversee the technological transition. The long-term goal for EMBs should be to build their capacity to self-administer all aspects of future elections, but initially it is likely that private vendors or technicians would need to be contracted to fulfill specific technological functions. In such cases, vendors' roles should be clearly defined, and the overall responsibility for administering the elections should remain with the EMB. The terms of the relationship with the vendor, as well as trainings and materials for election officials at all levels, should be open to observers so that they can assess the level of preparedness of the EMB.

Introducing electronic voting and counting systems will present the EMB with significant challenges in administering elections with the selected technology. Depending on the complexity of the technologies adopted and the existing technical competencies of the EMB staff, it is likely that new skill sets will be needed to administer the electronic systems. It is important that EMBs develop the capacity to administer as many aspects of the electronic voting and counting system as possible so that they maintain control over the integrity of the election itself. However, building the necessary capacity in various areas may be a gradual process.

Once the decision to adopt electronic voting and counting systems has been made, the EMB will need to designate who at the central level will be responsible for regulating, managing and operating these systems. While most EMBs have an IT department, assigning it responsibility for overseeing electronic voting and counting would likely overstretch the department's capacity, having a

potentially detrimental effect on the project. Instead, an EMB will likely need to create new structures to conduct these tasks.

An analysis of the staffing requirements associated with the project will need to be conducted as early as possible so that decisions can be made regarding whether the necessary competencies can be filled by training current staff or whether new personnel must be identified and recruited. The same issue will be replicated at the regional, local and polling station levels, in regard to both permanent staff and temporary election staff. Observers should be afforded access to such staffing plans, as these plans are critical to the successful implementation of new technologies.

It may be difficult for EMBs to recruit personnel with the necessary qualifications and experience to operate and update the new systems. EMBs may instead have to rely either on technicians provided by the equipment supplier or on the contracted services of private firms to fulfill specific technological functions, such as software programming and management of security features. Should such personnel be employed, their level of access to systems should be strictly defined and recorded, and their role should be transparent to observers.

Care should be taken to ensure that overall management of the systems remains within the EMB's authority, as it is responsible for the administration of elections and accountable to the public for their integrity. While private firms or other state actors may conduct important parts of the election process, they should not have overall responsibility for the administration of elections. Over time EMBs should prioritize building their capacity to administer all aspects of electronic voting and counting systems with their own staff resources.

Given the complex nature of electronic voting and counting systems, extended training of permanent and short-term personnel is likely to be necessary. Even at the polling station level, election officials must be knowledgeable enough

about the equipment they are required to operate in order to conduct basic troubleshooting if there is a problem on Election Day, or to correctly identify a problem so that the necessary technicians can be contacted. Polling officials must also understand the equipment well enough to explain the process to voters, which will help to increase public confidence in the systems. Similarly, training needs at the regional and central levels will also be significant, as officials must be able not only to operate the equipment, but also to solve problems and, in addition, must be able to explain the process to voters and other stakeholders.

Training for personnel at all levels, therefore, must be comprehensive and effective. Especially when voting and counting systems are used for the first time, it might be necessary for the equipment supplier to play a role in providing training. To the degree possible, the EMB should work with the supplier to develop the in-house capacity to conduct such training. For instance, the equipment supplier can conduct "training of trainers" courses for the in-house EMB trainers to gain the knowledge required to conduct the trainings themselves.

Training events and training materials should be open to scrutiny by observers and stakeholders. Observers should assess the effectiveness of the trainings and materials, and make any recommendations regarding improvements that may be necessary. Through such efforts, observers will also build their own understanding of the procedures and operation of the electronic voting and counting systems, as well as any possible weaknesses they should be aware of on Election Day.

KEY CONSIDERATIONS: RECRUITMENT AND TRAINING OF PERSONNEL

FOR IMPLEMENTING BODIES

- ☑ Has an analysis of the staffing needs associated with the project been conducted at both national as well as the regional, local, and polling station levels for staffing needs?
- ☑ Are levels of access to systems appropriately defined for external technicians that may be hired to assist in the process?
- ☑ Is training for personnel at all levels based on cooperation with the equipment supplier in order to develop in-house capacity to conduct trainings?
- ☑ Does the process include a training of trainers to build internal capacity?

FOR OVERSIGHT ACTORS

- ☑ Is the EMB staffing plan adequate for successfully implementing electronic voting and counting technologies, and are staffing plans made available to oversight actors?
- ☑ If outside technicians or consultants are involved, are their roles clearly defined and transparent?
- ☑ Do election officials, including at the polling station level, have sufficient understanding of the technologies, allowing them to clearly explain the voting and counting process to voters?

- ☑ Does the EMB have a long-term goal and plan to self-administer all aspects of electronic voting and counting in future elections?
- ☑ Do oversight actors, including parties and observer groups, have access to EMB trainings and training materials, allowing them to assess the adequacy of training, provide recommendations and build their own understanding of the technologies?