COLLECTION OF DATA

Creation of a voter list that is a "voter registry" independent from other registries (such as, the civil registry) involves collection of voter data by election authorities. However, rarely is an independent registry truly independent. There are almost always aspects that depend on the work of other institutions (e.g., the Ministry of Interior that issues ID cards or other proof of citizenship or the Transportation Department that issues driver's licenses, which are used by voters to prove their eligibility). Also, it is not unusual in these circumstances for the creation of the independent voter registry to be a one-time occurrence, and updates to be processed by some automated mechanism that requires sharing of data with institutions that are issuing birth, marriage or death certificates or some other means of recording the status of citizens.

It is important that monitors understand all manners of populating the voter database and recognize there will inevitably be some degree of error in creating the voter list. Database design and management processes should include "built in" tools to tackle this issue, but monitors should also look into what steps are taken to minimize, uncover and correct error.

This section will discuss issues related to the monitoring technologies used in the creation of the voter list, irrespective of whether the creation will be a one-time occurrence or continuous or periodic exercise, or whether it will be a voter-initiated or state-initiated process. What they all have in common is that the voters' data are not immediately recorded as electronic records in a central voter registration database and that fairly complex and sensitive operations must be used to collect and process these data.

Whether the collection of the data is done by direct or indirect recording, it is important to determine what type of information is being captured and whether this reflects the requirements of the legal framework. If election authorities are collecting data beyond what is required by the legal framework, this must be properly justified or discontinued. If election authorities are collecting data that will be shared with other governmental institutions, this should be disclosed.

Direct Recording:

Direct recording involves creating an electronic voter record at the moment and location when the voter (or his or her proxy) submits the data to the election officials in accordance with the law and regulations. In direct recording, voters do not fill out a form that will later be entered into the voter database by scanning or data entry in some remote location. Rather, their data is captured directly at the registration point using electronic equipment.

Development of the System. Observation of the direct recording technology must start at the point when election officials are developing specifications for hardware and software requirements. These requirements must match the model of the registration exercise — for example, mobile versus stationary registration points or a large number of points versus centralized locations. Equipment

requirements will differ if the equipment has to be transported or if it is stationary, if it relies on infrastructure (such as, electricity or networks) or if it is designed to work without infrastructure (for example, to run on batteries).

Software. Electronic records that the registration equipment creates must be compatible with the voter registry database so that records can be easily and accurately transferred to the central database. Principles discussed above, under "transfer of existing records" apply here too.

Testing. Direct recording equipment should be properly tested before it is deployed. Tests should be performed following the "end-to-end" principle, meaning that the complete process is simulated with actual components of the system and exact copies of the software in an environment that is similar, if not exactly the same as, the type where the equipment will be utilized. A complete testing and monitoring process requires recording data of people involved in the test at the actual registration points and transferring this data to the central database. In addition, "load tests" should be performed to gain a better understanding of how the equipment deals with the expected number of transactions and whether projections of the number of processed voters are realistic. Tests should also be conducted concerning how the database responds to malfunctions and problems.

Tests are performed not only to verify functionality of the equipment and the process, but also to examine usability of the system, both from the voters' and election officials' point of view. Beyond the functioning of equipment, authorities should solicit the opinions of all those involved in testing - simulated voters, officials handling equipment, supervisors and others. Monitors from political contestants and election observation groups should be allowed to provide input regarding any concerns they may have before tests are designed, review and ask questions about the testing procedures before they are conducted, witness all testing and be provided timely access to the opinions of all actors involved in the testing.

It is not expected that monitors from election observation groups or political contestants will perform these tests; however, they need to be able to evaluate how the testing was performed. Testing of the

systems is part of the electoral process. It requires that election officials have a clear test plan and that testing and outcomes are recorded and shared with monitors in a timely and understandable manner.

If tests are performed on a smaller scale, for example on a small sample of equipment, the tests are considered design tests or model tests. Performance tests are those that test the complete set of equipment. If the election officials do not perform a full scale performance test, it is necessary to establish criteria by which a sample of the equipment will be tested. The sample should be on a proper statistical probabilistic sample, where every piece of equipment that will be deployed to registration points has the same chance to be selected. Tests should not include just "the first 100 pieces of equipment delivered" or other arbitrary criteria because such tests have proven to be unreliable indicators of how the full set of equipment will perform.

Monitors from the political contestants and observer groups should be allowed to review sampling methodology. Monitors from observation groups and political contestants must thoroughly understand the system in order to evaluate whether performance tests can be reduced to test a sample of the equipment. Sometimes it is absolutely necessary to conduct full scale tests, especially if the equipment requires calibration and fine tuning (such as bio identification systems like fingerprint scans) or if it is impossible to troubleshoot problems once the equipment is deployed.

Accountability. As with every other aspect of the electoral process, direct recording of voter data should follow the principle of accountability. This means that every sensitive action should be recorded and stored to provide opportunities for possible examination. Since electronic records are not accessible to the public, individual voters cannot verify whether the equipment recorded their data properly. Therefore, direct recording registration systems must provide each voter with proof of her or his submission of their data. This proof can be a printout of the voter's record or some other type of receipt or certificate. Voters thereby are given an ability to prove their involvement in the registration process, which is usually needed in order to seek remedies should they discover errors or omission of their data.

In addition to the receipt that confirms submission of the data, the voter should receive a unique number for the transaction that will serve as an identifier. The receipt and identifier can aid voters in exercising their right to check the preliminary voter list and demand corrections if data is erroneously recorded or if the voter is somehow omitted from the list. The receipt and identifier also can aid election observation groups and political contestants to conduct independent verification exercises with the consent of registered voters, who agree to participate in such efforts.

Security, Back Up and Data Transfer Procedures. Security procedures should address two principal issues: (1) security of the data regarding unauthorized access and manipulation of data; and (2) security regarding potential loss and corruption of data. Election authorities should have defined security procedures that are made available for review by monitors from observation groups and political contestants. Monitors would not obtain security codes granting them access but would be able to comment on whether the procedures themselves seem adequate.

To ensure adequate security, data must be protected with technical and organizational solutions, and election officials should employ both methods to secure the data. Technical solutions are built in to the equipment and limit access to authorized election officials. Equipment must be tamper resistant or at least tamper evident. Technical security solutions should also have clearly identified access levels - not all of the officials should have access to all of the data and processes. Organizational solutions are a set of rules that election officials must respect to protect access to the system.

In order to protect data captured at the registration points, election officials must design a reliable back up process. Back ups have to be regular, scheduled and documented. Also, backed up data should be stored independently from the direct recording equipment, so that in case of malfunction of the equipment and loss of the original data, back ups are preserved. Storage and management of the back ups should also be included in design security procedures.

Monitors from political contestants and observer groups should also be allowed to evaluate procedures for the data transfer. Data transfer can be physical (e.g., by moving memory cards from the direct data

capture equipment to the central database) or through a computer network. Data transfers are sensitive points in the process since they pose a challenge to protection of the data by introducing elements of uncontrolled environments. Monitors should be allowed to accompany physical transfers or evaluate such transfers based on sampling techniques and should be allowed to evaluate transfer of data by networks through reliable techniques, such as comparing data sent from a particular machine or registration center (or sample of machines or centers) to corresponding data recorded centrally.

Development, Delivery, Maintenance, Troubleshooting and Service of Technologies. Ensuring the proper functioning of the direct recording equipment and related technologies—like every other aspect of election administration—is the legal responsibility of the election authorities. In effect, the election authorities have a duty to properly discharge the obligation of government to provide genuine democratic elections to the citizens, including to the voters and to those standing for election. It is common that election authorities outsource development and production of the technologies to independent companies, and they often rely on the private companies (that many times are foreign entities) to deliver, maintain, service or otherwise troubleshoot problems with the technologies. This normally creates a legal contractual relationship between the election authorities and equipment producers (vendors) and/or servicers. However, that legal relationship is subordinate to the election authorities' legal obligation to citizens, which is set by the country's constitution, electoral law and often reinforced by international human rights obligations.

The role of the equipment producers and/or servicers and the capacity of the election officials to service equipment is an important consideration in ensuring electoral integrity. The importance of building capacities of election authorities and avoiding over-reliance on vendors is essential to meeting a government's obligations to organize genuine democratic elections. Delivery of equipment should be complemented by the transfer of know-how to electoral authorities to effectively service the technologies, or electoral authorities must ensure that producers and/or servicers are in-country and in position to provide effective service that allows the technologies to perform according to the registration plans. Otherwise, the entire voter registration process can be jeopardized.

Contracts therefore should be open to scrutiny by observation groups and political contestants.

COUNTRY NOTE:
Nigerian Elections 2007 - Use of Electronic Technologies in Voter Registration

While the Nigerian electoral act prohibits electronic voting, the Independent National Election Commission (INEC) decided to employ direct data capture (DDC) devices to create an entirely new voter registry for the series of elections held in 2007. DDC technology would have enabled officials to electronically enter and store information about each voter who appeared at registration locations and then transfer the information to a computer database. Election authorities would then have been able to conduct various checks to ensure the integrity of voter lists, for example, to identify duplicate records and thus prevent double voting. However, the INEC's very tight and optimistic timetable proved not to be realistic. INEC expected to procure from three companies a total of 33,000 DDC machines by early November in order to complete registration of an estimated 70 million eligible voters by the December 14 legal deadline. At the beginning of registration only about 1,000 DDC machines were operational, and due to a number of factors, including delayed payments to the vendors, the 33,000 machines were not in place until mid-January. Only about 5,000 of the machines were voter registration devices, while the majority of machines used were laptop computers with digital cameras. In addition, registration staff apparently did not receive sufficient training on the use of the DDC devices. The batteries provided had a short life span and recharging facilities were limited in number, often rendering the DDC devices unusable. The printers frequently jammed, and there were shortages of ink. A manual registration process had to be used as back-up. The result was significant delays beyond legal deadlines, a problematic correction period, which led to likely disenfranchisement, and opportunities for illegal voting due to inaccurate voters lists. While aggregate registration figures were made public, there were questions about the large volume of registrations in the final phase of the exercise. Public confidence was further compromised because significant access to the voters list was not provided to political parties or domestic and international observers prior to election day. Eighteen political parties joined in a court challenge concerning noncompliance with legal provisions on voter registration.

Sources: "NDI Final Report on Nigeria's 2007 Elections,"; "Nigeria Final Report: Gubernatorial and State House Elections 14 April 2007 and Presidential and National Assembly Elections 21 April 2007," European Union Election Observation Mission.

Obligations of the producers and/or servicers after delivery of the products should be clearly defined by contracts that carry an appropriate level of guarantee that the producer will indeed effectively service the equipment. The contracts should address obligations to effectively remedy breakdowns of equipment due to design flaws, as well as due to operation in high temperatures, high humidity, exposure to sand particles, failures of batteries needed to operate equipment as specified; and the ability to rapidly provide replacement parts and otherwise ensure equipment performance. The schedule for delivery of equipment needed to meet the election

authorities' voter registration plan should be verified against the producer's available inventory and production schedule (including obligations to deliver equipment and technologies to other countries). All of these issues have had serious negative effects on voter registration processes and must be taken into account.

It must be expected that something will go wrong during registration of voters. Tests should help to identify and minimize weak points and reduce malfunctions, but officials must expect and plan for problems. A bigger problem than failure of some components is not having an effective response plan. Response plans must be clear and documented. They must define response steps, response times and roles. If the response involves the equipment producer or another contracted company, this should be clearly defined in valid contracts. Such response plans should be made available to observer groups and political contestants, with opportunity for their comment. This is an important point for genuine transparency and confidence building.

Training. Election officials who perform voter registration should be trained in verification of the voter's eligibility, in how to properly record the data and in how to otherwise operate the equipment. They must understand the functioning of equipment (technologies) on at least a basic technical level in order to identify problems, to be prepared to correct them on the spot, if possible, and to request appropriate assistance and service.

The training should be in line with standard training requirements - trainings should be thorough, mandatory, standardized and include simulations of normal procedures and responses to malfunctions. Monitors from observer groups and political contestants should as a best practice be allowed to review training plans and materials before they are employed and to provide comments. Monitors should in any case be allowed to attend and observe training sessions to build confidence in how officials will be prepared to use technologies during the voter registration process.