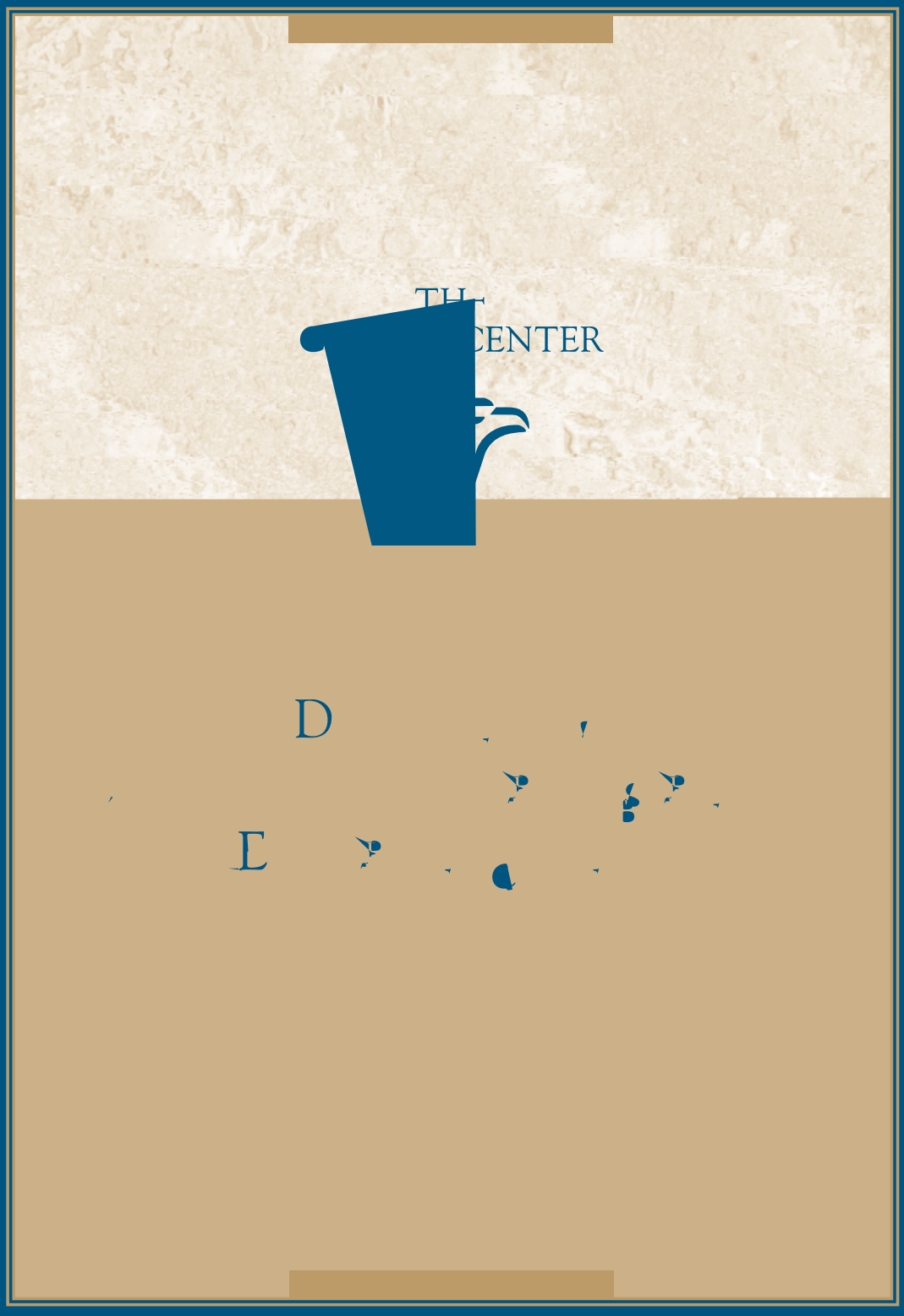

Waging Peace. Fighting Disease. Building Hope.

The increasing use of new electronic voting (e-voting) technologies in elections around the world has been recognized by the international election observation community as one of the paramount challenges facing election observation today. As a whole, international election observation organizations have had relatively little experience observing elections in which e-voting technologies are used. In addition, the inherent lack of transparency of electronic voting technologies discourages easy observation.

E-voting systems thus pose important and unique challenges for election observers: How can observers assess the workings of electronic systems where the

between different equipment and software and different physical locations. The next several sections summarize the main points of Dr. Jones' presentation and the discussion among meeting participants.

Election cle

Pre-election tests and audits are an optimal opportunity for international election observers to assess not only the functioning of the electronic voting system but also the access of key stakeholders to the electoral

There are two components for providing proper security during the various exchanges in the cycle: physical security and technical security. Physical security measures often include documented chains of custody to certify that each person involved in the process performed the proper protocol for the delivery and transfer of equipment and data. Technical security, on the other hand, usually involves cryptography to ensure that the software and the machines cannot be tampered with. The need for observers to focus exclusively on technical security measures generally occurs only if the physical security procedures have proven inadequate.

The methods used for transferring data from the polling centers to the tabulation center and for finally tabulating the votes can also present a significant

Prior to the November 2006 meeting, The Carter Center developed a draft methodology for observing the use of electronic voting technologies. This draft methodology served as the basis for discussion during the workshop. As outlined above, the principal activities of the Center's two-year initiative on e-voting include a series of collaborative workshops and meetings, and pilot missions in collaboration with representatives of other observation groups, aimed at refining the methodology and increasing the hands-on experience of international observers with electronic voting. The following section provides an overview of the methodology and highlights the guiding principles that were identified during the November 2006 meeting discussions.

In electronic voting processes, observers are faced with trying to verify election processes that are at times opaque or occurring within a so-called black box. Observation of electronic voting technologies must, first and foremost, be concerned with assessing whether electronic voting technologies uphold international standards for democratic elections, such as the secrecy of the ballot and the right of the voters to participate in government. Recognizing that election day observation alone does not permit a complete assessment of whether these rights are being fulfilled, the Carter Center methodology takes a broader approach to the observation of electronic voting.

As with traditional election observation, observation of electronic voting must begin well in advance of election day and should consider the broader electoral context, such as the legal framework for the elections, voter education, poll worker training, political campaigns, and so forth, as well as the events of election day. Furthermore, because many tests, audits, and preparations of the electronic voting equipment take place months in advance of election day, observation of electronic voting requires additional emphasis on long-term observation and documentary research.

The use of electronic voting technologies also widens the scope of focus for observers in that it introduces new stakeholders into the electoral process, such as certification bodies and vendors. To understand the impact of technologies on the quality and conduct of the elections, observers must consider new types of information that would not necessarily have been included in traditional observation approaches, such as the contractual relationship between the election management body and the vendor.

In order to develop a standard methodology that can be applied in a wide variety of circumstances and to a variety of technical solutions, the Carter Center's draft e-voting observation methodology aims to identify key issues and questions to be assessed. The draft methodology includes generic template forms that allow the methodology to be usehe 91 -1euber 2f tdif1(-)TJT*(tfre

The baseline survey used in the Carter Center draft methodology contains 144 questions intended to guide the observation and assessment of the user. The information gathered by answering these questions, based on interviews with stakeholders and the review of legislation, rules, regulations, and other pertinent documentation, should help the observation team create a comprehensive picture of the voting system in use and how it should work and thus allow a more complete assessment. In this observation model, the baseline survey would be completed by long-term observers and core team members, such as the field office director and in-country staff, with assistance where necessary from technical experts in the months leading up to the election.

After collecting as much data as possible, the core team will produce a synopsis of the findings, providing an overview of the system that can be used by the team and by short-term observers. In addition, this information will be used to modify more generic election day and other checklists so that they become effective tools for capturing the observations of the team on how the system actually works in practice.

The baseline survey includes questions on eight general aspects of the electronic voting system: (1) the legal framework; (2) technology vendors and procurement of equipment; (3) certification, testing, and security of the system; (4) public confidence in electronic voting technologies; (5) voter accessibility; (6) election day procedures; (7) contingency planning; and (8) ballot counting, recount, and complaints procedures.

Legal Framework

As with any election, consideration of the legal framework regulating the electoral process is essential to a full understanding of it. A thorough review of the legal framework will help observers assess the degree to which the state has sought to provide not only clear and consistent rules and regulations for all aspects of e-voting and any reasonable eventuality that may arise from its use, but also the degree to which the state has taken clear steps to protect the internationally recognized rights of voters to cast a secret ballot, participate in their government, and have their vote counted as cast. In addition, review of the legal framework will help observers gauge the degree to which the election management body is taking active steps to promote transparency in the electoral process through mechanisms such as audits, impartial and independent certification, and testing.

In particular, Carter Center observers consider the roles and responsibilities of key stakeholders as outlined by law and focus specifically on the legally enforceable accountability of stakeholders—both traditional stakeholders such as election management bodies and nontraditional stakeholders such as certification bodies, vendors, and contractors. In addition, observers consider the degree of access granted by the legal framework to domestic observer groups and political party agents in addition to members of international observation delegations. While this is a critical aspect of observation of any election, the opacity of elections in which electronic voting technologies are used makes it critical that observers gain a sound understanding of these issues.

Technology Vendors and Procurement of Equipment

Electronic voting vendors and the systems they produce may be selected for a variety of reasons. Transparency and accountability in the tendering and procurement processes are critical to ensuring that the rights of voters are not undermined by private interests.

By asking the questions outlined in the Technology Vendors and Procurement of Equipment section of the baseline survey, observers will better understand the reasons why election management bodies have chosen to introduce electronic voting technologies, why they have chosen a specific technical solution, and how transparent the tendering process is. In addition, this section of the survey will guide observers in their consideration of the role of vendors in the electoral process, a role that in traditional elections may not be as important. In particular, Carter Center observers focus on the nature of the vendor's relation-

ship with the election management body and other key stakeholders to ensure that the relationship is free of conflicts of interest and that there was a competitive and transparent tendering process that resulted in the selection of a particular vendor to provide e-voting equipment and related services.

Certification, Testing, and Security of the System

The Certification, Testing, and Security of the System section of the baseline survey includes several critical issues that observers must consider to gain a sound understanding of the system, including voter verified paper trails and audits, certification, testing, physical security, software, integrity of the system, and ballot building.

ote e i ie lP e il n it

One widely accepted means of ensuring that the electronic voting system is recording votes as they were cast by voters is the use of a voter verified paper trail (VVPT). A VVPT allows a voter to cast a ballot electronically and then verify that the machine has accurately recorded the vote by checking a machine-produced paper receipt that captures the choice. This paper receipt should then be placed in a secure ballot box that protects the secrecy of the vote and can be manually recounted after the election. The results of the manual count can be compared to the electronic results produced by the machine (see the case of Venezuela, outlined in the next section of this report). Voters should not be able to remove the ballot paper or other proof of how they voted from the polling place.

Comparisons between the paper receipt count and the electronic results are useful for ensuring that the machine is accurately recording the voters' choices. If such comparisons are conducted on a statistical sample of machines, the sampling method must be clear and be consistently applied and follow sound statistical sampling practices to produce meaningful results that can be extrapolated to the universe of machines in use. In addition, observers should consider whether the results of the paper count can be used as the basis for a legal challenge to the election results.

e ti ic tion

Impartial, independent, and transparent system certification measures should be in place to ensure that the system meets national or international standards, the requirements of the election jurisdiction, as well as the technological specifications outlined by the vendor. International election observation missions should not be responsible for the certification or testing of an electronic voting system. Because this responsibility lies with election management bodies and the organizations with whom they work, Carter Center observers assess the functioning of the certification body and its relationship with other key stakeholders in the process, including the election management body, political parties, the vendor, and others. Questions included in this section of the baseline survey are intended to help capture data about the transparency, independence, and impartiality of the certification body and help observers understand any financial relationships that the certification body may have with the government, political parties, and others that fall outside the bounds of the contractual agreement between the certification body and the election management body. Observers also assess the degree of access granted to political party agents and observers, both international and domestic, in the certification process.

e tin

Electronic voting systems, including equipment and software, should be tested prior to the deployment of voting machines on election day to help ensure that the machines work as anticipated. This testing should be conducted in an impartial and transparent manner and should include all aspects of the system. Carter Center observers should gather information that will help assess the impartiality, independence, and comprehensiveness of the testing scheme in place.

lP ic l ec it o t e te

As in a traditional election, the physical security of election materials is an essential measure for protecting the integrity of the election, regardless of the technical solution used. Election management bodies should have clear processes and procedures in place

that regulate physical access to the equipment, document such access, and prevent physical tampering with the machines. Included in these processes should be mechanisms that allow any tampering to be evident (such as seals over data ports) and clear regulations outlining procedures to be followed if tampering is discovered. Voting materials, including electronic voting equipment and backup paper ballots, must be kept in a secure location at all times and should remain secure throughout transportation. Using the baseline survey and other forms, Carter Center observers collect information about the processes and procedures in place to regulate physical access to all electronic voting equipment and the central tabulating computers.

o t e

The software used in electronic voting systems should be subject to impartial and transparent inspection. Inspection of the software by an independent body or by independent inspectors should be required by the election management bodies. Observers, both domestic and international, should have access to documentation detailing these inspections. Carter Center observers should collect data, through the baseline survey and other forms, to understand the nature of the software inspection, including who conducts the inspection, the conditions under which the inspection takes place, and what the inspection includes.

llot il in

The construction of electronic ballots is generally based on the creation of complex databases. The nature of this process introduces a high possibility of human error. Clear policies and procedures regarding the creation of electronic ballots, including institutional roles and responsibilities, are helpful. Ballots should be consistent in layout and design with any paper ballots that may be used.

nte it o t n i ion

The need to ensure the security of the system also extends to the transmission of the data from the voting machines in the polling place to the tabulating computers. Steps should be taken to effectively protect the transmission of data and prevent illegal access, or hacking. Observers should collect data that will help the observation mission assess the extent to which steps have been taken to protect the integrity of the data transmission.

Public Confidence in Electronic Voting Technologies

Allowing domestic observation groups, political party agents, and the public to have access to the electoral process, including those aspects that are automated, is a critical means of promoting public confidence. In addition, it is often helpful for electoral management bodies and legislators to include all stakeholders (e.g., civil society organizations, political parties, and voters) in the selection and introduction of new electoral technologies. This should include training for voters, political party agents, domestic observers, and others on the technologies, covering how to use them and how to assess indications of possible technology failure. Carter Center observers should assess the extent to which there is public debate about the use of electronic voting technologies, the degree of stakeholder participation in the automation of the electoral process, and, where possible, the steps taken to ensure that there is a high level of public comfort with the technologies in use.

Accessibility

To ensure that voters are not disenfranchised by the introduction of electronic voting technologies, election management bodies should take steps to check that all qualified voters are able to cast their ballots. This includes those who are disabled, illiterate, or do not speak the majority language of the country. Observers should consider the provisions in place to protect the right of these voters to cast ballots, including ballot design (e.g., in minority languages) or availability of ballots in larger type sizes, the availability of electronic voting machines for disabled voters, and any provisions to ensure that illiterate or disabled voters are able to cast and verify their votes.

Election Day Procedures

As in any election observation mission, it is important for observers to gain a comprehensive

understanding of procedures for elections in which electronic voting technologies are used, including voting processes. Electronic voting technologies should offer voters the same options as manual voting, including, but not limited to, casting blank ballots and cancelling their votes. If a voter verified paper trail (VVPT) is used, a voter should be able to cancel his or her vote should the paper receipt not reflect the ballot cast on the machine. Steps also should be taken by the electoral management body to ensure that the secrecy of the vote is protected, that a vote cannot be traced back to a specific voter, and that voters are not able to remove evidence of how they voted from the polling place.

Contingency Planning

Election management bodies should have clear and consistent rules in place in case of machine failure, whether resulting from power outages or other issues. These rules should be clearly communicated to all poll workers and technicians as well as observers and party agents, and poll workers should receive training on what to do in such instances. Any machine failures should be clearly documented. Documented chain-of-custody procedures should be in place to ensure that machines are secure from tampering once removed from the polling station either at the end of polling or in case of machine failure. Any replacement equipment should be subject to the same testing and certification processes as equipment initially installed in the polling place. International observers should assess the degree to which election management bodies have taken steps to ensure that contingency plans and procedures are clear to election officials and are implemented throughout the electoral process as well as what these plans and procedures are.

Ballot Counting and Recount and Complaint Procedures

The use of electronic voting technologies, particularly those that do not produce a VVPT, poses unique challenges to the observation of ballot counting. Regardless of whether the machines produce a VVPT, election results should be printed at the station level prior to transmission to the central tabulating computer, allowing the public and observers, at the very least, to conduct a comparative assessment of the

- While the CNE managed to address some of the opposition's concerns, doubts remained about the use of the automated fingerprint identification system (AFIS). In the past, the opposition suggested that the fingerprinting machines could compromise

Another concern of the November 2006 meeting participants was the limited access to the source code that was provided to the non-CNE/Smartmatic technicians participating in the audits. In Venezuela, auditors were allowed to review the source code

cast their votes with little impediment. Nevertheless, some details related to the design of the machines were observed, such as confusion among voters regarding the paradigm shift between choosing a candidate using the touchpad and choosing to cast a blank ballot on the touchscreen. Another issue observed was the apparent lack of procedures for vote correction should a voter allege that the printed paper slip does not reflect his or her choice. In addition, the Center observed certain design characteristics that could make it difficult for illiterate people to cast their votes and limited the amount of time allotted for each voter to cast his or her ballot.

The mission found that the CNE took reasonable steps to secure the machines, including the encryption of the voting information stored in the machine memories, the use of randomization mechanisms to prevent vote sequence reconstruction, and implementing paper receipt security measures.

In addition, the CNE put in place a number of procedural safeguards to promote the physical security of the machines, including chain-of-custody measures intended to ensure that the machines cannot be tampered with. The Carter Center team noted several minor incidents that suggest confusion among table authorities and Plan Republica officers regarding the protocols for tamper prevention and a lack of clear and consistent guidelines for all election staff. While these incidents do not prove that any manipulation occurred, they do show that it is theoretically possible. Therefore, future elections would benefit from greater procedural clarity and a consistent application of election protocols.

The Carter Center team found that the CNE has taken important steps to protect the electronic system against outside attacks on the integrity of votes once they are stored in the machines and the transmission of votes from the voting machine to the tally center. The mission found it more difficult, however, to evaluate the degree of security against potential internal attacks on the system, which are possible in any electronic voting system, or the degree of security in the central tally system. Notwithstanding, The Carter Center team believes that the system would benefit from additional layers of security that could protect it from potential internal vulnerabilities.

Venezuela implemented a large number of audits in the three months preceding the election, on election day, and in the immediate postelection period, including hardware and software audits.

In the months following the November 2006 meeting and the December 2006 pilot mission to Venezuela, The Carter Center has reached the following conclusions about the draft methodology and plans to amend it accordingly in advance of subsequent missions and workshops:

- Checklists should include questions to capture data on the broader environment in and around the polling station.
- Observation of the legal framework is an essential component of the observation of electronic voting technologies. In particular, observers should focus on whether the law has mechanisms in place to ensure that the secrecy of the ballot is protected and that votes are counted as cast.
- Where possible, observers should observe pre-election tests and audits, noting whether access to these audits was granted to key stakeholders such as political party agents and domestic observers. This may also include whether observers were able to audit the source code and what the parameters for the audit included (e.g., whether observers received hard copies of the code and were able to review it with pencils).
- The data collected by using the baseline survey proved to be voluminous; however, it provided a fairly comprehensive overview of the system in use. Based on the amount of information involved and the subsequent task of report drafting, The Carter Center should include a longer technical appendix to the final reports of comprehensive missions so that reports are not unwieldy.
- Within the baseline survey, greater emphasis should be placed on collecting data related to the tabulation process.
- In addition to standard postelection debriefing, the Center should devise templates for election

4. Is this the first time these technologies have been used?

5. If no, how long have e-voting systems been used? In which previous elections were they used? Please provide separate reviews of previous elections.

6. Are there any documents available to the public containing information on the version numbers, makes, models, and functional status of these technologies? If so, please attach any relevant reports.

7. Does the technology produce a voter verified paper trail? If yes, please describe how it works.

8. Is the voter able to verify that the paper ballot matched his or her choice *before* the vote is cast?

9. Describe what happens to the paper trail during and after voting.

10. Provide an overview of the institutions responsible for the administration of the electronic voting systems, including the vendor, any certification or testing bodies, and organizations responsible for maintenance or election official training.

11. Do these organizations provide checks and balances on one another? If so, please explain how they do so.

12. Please include a diagram, detailed descriptions and, where possible, photographs of the election office components; how they are connected to one another; and their respective roles in the election process.

13. Provide detailed descriptions of the devices used in each polling place (e.g., DREs, supervisor's cards, voter's cards, memory cards), including physical descriptions, photos (if possible), descriptions of how they work, and when and how they interact with one another.

14. Please include a detailed diagram and description of how the different technologies used are networked.

Legal Framework

15. Is the use of electronic voting technologies anticipated in the current electoral legislation (or other binding legislation) or has it been introduced via subsequent decree, regulations, or other ad hoc measures?

16. Does the legal framework prescribe the type of electronic technology that is used? If so, please describe, including any outlined objectives for the introduction of this technology.

17. Does the law (legislation or subsequent decisions, decrees, and regulations) provide for transparency promotion measures, such as the use of an independent certification body and pre- and postelection audits that are open to party agents and observers? If so, please describe and indicate whether, in your opinion, access of party agents and observers to the audit process appears adequate.

18. Does the law (legislation or subsequent decisions, decrees, and regulations) require that appropriate technical steps be taken to ensure that the secrecy of the vote is guaranteed (for example, measures to ensure that the voting sequence cannot be reconstructed or that the votes cast cannot be tied to a specific voter)?

19. Does the law (legislation or subsequent decisions, decrees, and regulations) clearly outline the roles and responsibilities of public authorities, independent bodies, and vendors? Please describe.

20. Does the law (legislation or subsequent decisions, decrees, and regulations) provide a framework for contractual obligations between the state and the vendor or the independent certification bodies that is unique from standard contract law? Please describe the regulatory framework for these relationships.

21. Does the law (legislation or subsequent decisions, decrees, and regulations) make special provision for complaints and remedial actions based on the use of electronic technologies? Please provide a detailed description of the provisions and how they are related to the standard complaints procedures.

22. Do electoral offense provisions of the electoral law also apply to the new technologies in use?

Technology Vendors and Procurement of Equipment

23. If e-voting systems have been recently introduced, why were they introduced?

24. Who designed and developed the electronic voting system? Was the technology designed by the state or the vendor?

25. What vendors provide which components of the electronic voting systems? Please describe.

26. Is the technology leased or purchased?

27. Have the above vendors made contributions to political parties or campaigns? If so, please describe and attach any relevant documentation.

28. At what level was the procurement process of this technology initiated and conducted?

29. Was the vendor chosen through a transparent and competitive process? Please describe and attach any supporting documentation.

30. What reasons were given by those responsible for this choice of technology?

31. Are any of the following services included in the contract with the vendor? If so, please explain in greater detail.

    a. Timely supply of equipment
    b. Pre- and postelection testing
    c. Regular physical maintenance
    d. Regular software upgrades
    e. Replacement of equipment in case of failure
    f. Ballot design
    g. Ballot printing
    h. Warranties
    i. Other (please describe)

32. What, if any, penalty or reimbursement provisions are triggered by technical problems with the technology?

Certification, Testing, and Security of the System

33. If the machine produces a VVPT, is the voter able to verify that the paper ballot matched his or her choice *before* the vote is cast?

34. What happens to the paper trail during and after voting?

35. Do rules and regulations ensure that the VVPT does not undermine the secrecy of the ballot and that voters are not able to remove evidence of how they voted from the polling station?

36. Is certification of the voting technology required by law (legislation or subsequent decisions, decrees, and regulations)?

37. What is the certification process? Please describe the process in detail, including the relationships between the different certification processes, and attach any relevant documentation.

38. Who is responsible for this certification?

39. Who pays for the certification of the technology?

40. What is the relationship between the certification body and the organization whose technology is being certified?

41. Does certification occur before or after the procurement process?

42. Is the certification process accessible to the public, political party agents, domestic observers, or international observers?

43. What standards are applied to the certification of e-voting technologies? Please attach relevant documentation.

44. Is the technology recertified after every upgrade and repair?

45. In your opinion, after systematic review, what are the weaknesses of the certification standards?

46. Does the law require that acceptance testing take place?

47. Which components of the system undergo acceptance testing?

48. What does acceptance testing include? Please describe.

49. Who is responsible for acceptance testing?

50. Who designs the acceptance tests?

51. How often and when do acceptance tests occur?

52. Who pays for acceptance testing?

53. Who has access to the acceptance tests?
    a. General public
    b. Political party agents
    c. Domestic observers
    d. International observers

54. Under what conditions are acceptance tests conducted?

55. Does the law (legislation or subsequent decisions, decrees, and regulations) require that pre-election testing take place?

56. Who is responsible for pre-election testing and does the law (legislation or subsequent decisions, decrees, and regulations) require that the equipment is tested publicly and by an independent body? Please explain these procedures, including who is allowed to observe testing.

57. Does the state have recommended procedures for the testing and use of each type of election equipment? If so, please describe these procedures and attach any supporting documentation.

58. Who designed the pre-election tests?

59. Who conducts the pre-election tests?

60. How many machines are tested? Please provide details of the sampling method used to conduct the pre-election tests.

61. What is the timetable for pre-election tests and where are they conducted (in a central location, provincial locations, or elsewhere)? Please provide further details and any relevant documentation.

62. Is equipment retested after every upgrade and repair? If not, why?

63. Are pre-election tests open to the general public, political party agents, domestic observers, or international observers? Please attach relevant documentation.

64. Is all voting equipment tested upon delivery from voting technology vendors?

65. Does the law (legislation or subsequent decisions, decrees, and regulations) require that pre-election testing include the following?
    a. Testing the power-up of every machine
    b. Simulation of likely voting orders, patterns, and ranges

c. Stress-testing with large numbers of votes
d. Checking vote tally
e. Testing correct date and time information
f. Testing date set to election day run-throughs
g. Simulations of error conditions to evaluate system response to problems and mistakes
h. Testing reboot and restart functionality
i. Testing equipment recovery from system crashes
j. Testing for unexplained flashing or otherwise inconsistent or potentially suspicious behavior
k. Checking for complete list of candidate names, party affiliations, ballot initiatives, or proposition options
l. Testing the use of an independent log to compare the system count and the selections made by the voter
m. Testing the use of an independent log to compare the paper ballots (if used) produced with the system count and the selections made by the voter
n. Testing of display calibration
o. Testing of audio ballot functionality
p. Testing of the security and authentication techniques used in connecting the voting machines to the network (if applicable)
q. Testing to ensure that the ballot information for each precinct is correct
r. Other (please describe)

66. Please provide any relevant documentation outlining the regulations and procedures for pre-election testing.

Election Day Testing

67. What tests or audits, if any, are required on election day? Please describe in detail and attach any relevant documentation outlining regulations and procedures for election day auditing or testing.

Physical Security of the System

68. Please provide a detailed description of the technologies in place to ensure the physical security of the electronic voting system (e.g., tamper-evident seals).

69. Who is allowed physical access to the equipment, and what measures are taken to prevent physical tampering with election equipment?

70. Is physical access documented? If so, who maintains these records?

71. Are vendors permitted access to the voting systems after they have been delivered? If so, for what purposes and when are they permitted access? Is this access controlled and documented?

72. What happens if a machine is found to have been tampered with? Please describe any contingency plans for such an event.

73. Who is responsible for transporting the machines from their storage location to testing centers and polling places? Please provide relevant documentation.

74. Is the chain of custody during the transportation process documented? If so, who maintains those records?

75. When will transportation of the equipment take place?

76. Who pays for the transportation of the equipment?

77. Are records kept of all upgrades and repairs made to voting equipment?

78. Is any equipment used for a purpose other than election administration? If so, please provide further details of the other uses of the equipment, including the purpose, how people have physical access, other software that is required for this secondary use, and so forth.

79. Which components of the system are stored in escrow?

80. Are there written procedures and requirements regarding the storage of voting system software stored in escrow? If so, please provide further details on these requirements and the people who have access to the software.

81. Is there a cutoff date after which no further changes or updates may be made to the voting system? What is that date?

82. Please provide a detailed description and diagram of all of the data paths in and out of the components of the system.

83. How is access to the data ports secured when the equipment is not in use?

84. What is the method of transmission of information between the technologies? Please describe.

85. How are transmissions secured from alteration and interference? Please provide a detailed description.

86. Is any of the voting system software open source software? If yes, please include information on location and availability.

87. Who is responsible for inspecting the software used in the electronic system?

88. Under what conditions does the official software inspection take place? Please provide a detailed description of the software inspection process, including the length of time allotted for the inspection and the means of inspection.

89. Does the law (legislation or subsequent decisions, decrees, and regulations) allow independent inspection of the software? Please provide further details, including any pertinent reports that might be available.

90. Under what conditions are independent software inspections (including representatives of political parties and civil society) conducted? Please provide a detailed description of the inspection process, including the length of time allotted for the inspection and the tools inspectors are allowed to use.

91. Does the software inspection (either by an independent body or the official organization responsible) include checking the source code against the executable code?

92. Who is responsible for creating the executable code from the source code, and is this process subject to independent verification?

93. Is any extraneous software installed on the servers? If so, please provide further information about this software and its use.

94. Who has physical access to the central tabulating computer, and what measures are taken to prevent physical tampering with election equipment?

95. Is physical access documented? If so, who maintains these records?

96. Are vendors permitted access to the central tabulating computer? If so, for what purposes and when are they permitted access? Is this access controlled and documented?

97. Are records maintained of all upgrades and repairs made to the central tabulating computer?

98. Is the central tabulating computer used for any purpose other than election administration? If so, please provide further details of the other uses of the equipment, including the purpose, the people who have physical access, other software that is required for this secondary use, and so forth.

99. Are there procedures in place that encourage independent verification of the transmission of data (such as printing of polling place election results prior to transmission to the central tabulating computer, which can be compared to the final or interim results)?

100. When is this computer networked to the other hardware in use?

101. Please describe in detail and provide diagrams of all of the data paths into and out of the central tabulating computer.

102. Is the transmission of information between the central tabulating computer and other equipment secure from any outside intervention or hacking? Please describe security measures in place.

103. What contingency plans are in place in the event of failure of the central tabulating computer? Please describe.

Accessibility

121. Are ballots available in minority languages?

139. Who is financially responsible for the cost of a recount? Please provide further information, including whether an individual, if financially responsible, can seek reimbursement for the cost.

140. Are paper or electronic ballots recounted? If paper ballots are recounted, were these ballots verified by the voter? Please provide a detailed description of this process.

141. What voting records are maintained?

    a. Paper ballots
    b. Electronic records stored in the hard drive or disk on module (DOM) of the machine
    c. Electronic records produced by the modem
    d. Records maintained in a secondary memory device

142. If multiple records are maintained, are these reconciled as part of the counting or recounting process? If yes, please describe.

143. In case of discrepancy, what is the ballot of record? Please provide further details.

144.

Polling Station No.: _____

TT

	Direct Observation		Reported to Our Observers		Not Observed or Not Applicable	
c. If the machine was not replaced within 120 minutes, did the polling station change to manual voting?*	Yes	No	Yes	No	N/O	N/A
13. Did you observe the machines to be free from any irregular interference such as the connection of an external keyboard or any other device (except the						

Poll Opening—Electronic Poll Book Observation

	Direct Observation	Reported to Our Observers	Not Observed or Not Applicable
24. Is the automated fingerprint system going to be			

E D *ene el*

Instructions:

If you cannot answer the question because you have not observed this aspect of the electoral process, please circle N/O — Not Observed. If the question is not relevant, please circle N/A. If you answered "no" to any asterisked (*) question or irregularities occurred, please provide details on the back of the form.

When possible, ask domestic observers and political party agents for their observations during the period prior to your arrival. When applicable, fill out both the "Direct Observation" and the "Reported to Our Observers" columns, even if the responses are different.

Polling Station No.: _____

Team No.: _____ Time of Arrival: _____

City/District: _____ Time of Departure: _____

Province: _____ Date: _____

1. What technology is used in this polling station?

a. Smartmatic SAES 3000 voting machine (small DRE)	
b. Smartmatic SAES 3300 voting machine (larger DRE)	

2. How many machines are located in this polling station? _____

	Direct Observation		Reported to Our Observers		Not Observed or Not Applicable	
17. Are paper ballot receipts handled according to the established procedure?*	Yes	No	Yes	No	N/O	N/A
18. Are the machines' ports physically closed and inaccessible during voting?	Yes	No	Yes	No	N/O	N/A
19. Is the equipment free from network connectivity throughout your observation?*	Yes	No	Yes	No	N/O	N/A
Handling Exceptions—Please Address the Following Questions to Polling Officials						
20. Are poll workers aware of contingency plans in case of equipment or system failure?*	Yes	No	Yes	No	N/O	N/A
21. Is replacement voting equipment (machines, cards, card programmers, etc.) available in the event of failure?*	Yes	No	Yes	No	N/O	N/A
22. Is the same equipment set up at poll opening used throughout the day?*	Yes	No	Yes	No	N/O	N/A
23. If no, is the chain of custody for the removed equipment documented?*	Yes	No	Yes	No	N/O	N/A
24. If voting equipment is taken out of service during election day, are votes and other relevant information extracted from it?*	Yes	No	Yes	No	N/O	N/A
25. Is there documentation outlining the failure that has occurred and recording the chain of custody for:						
a. The machine?*	Yes	No	Yes	No	N/O	N/A
b. The information drawn from the machine?*	Yes	No	Yes	No	N/O	N/A
26. In case of power loss can the equipment operate on a battery?*	Yes	No	Yes	No	N/O	N/A
27. If yes, do polling officials:						
a. Have sufficient batteries?*	Yes	No	Yes	No	N/O	N/A
b. Know the average life of the battery?*	Yes	No	Yes	No	N/O	N/A

Polling Station Officials

	Direct Observation		Reported to Our Observers		Not Observed or Not Applicable	
28. Have polling station officials received training specific to the equipment in use, including trouble-shooting in case of technical difficulties?*	Yes	No	Yes	No	N/O	N/A
29. Are polling station officials adequately instructing voters on the method for casting their ballots?	Yes	No	Yes	No	N/O	N/A

Election Day Auditing

30. Did polling officials conduct parallel testing?*	Yes	No	Yes	No	N/O	N/A

Comments

2. Which communication method is being used in this polling station?
   a. Fixed-line telephone ☐
   b. Cellular telephone ☐
   c. Satellite telephone ☐
   d. No transmission, but transport of memory stick to nearest transmission center ☐
      To which center? _____

3. How many machines are located in this polling station? _____

4. What is the number of registered voters in this polling station? _____

5. Where were these machines stored immediately prior to the election?

   _____

   _____

6. When did the equipment arrive at the polling station?

   _____

   _____

[illegible]

The Carter Center, Atlanta, Ga.

o

Participants

Eric Bjornlund
Democracy International

Michael Boda
Consultant, The Carter Center

Julia Brothers
National Democratic Institute for International Affairs

Andrew Bruce
European Commission

David Carroll
The Carter Center

Ray Cobb
Center for Election Systems, Kennesaw State University

Avery Davis-Roberts
The Carter Center

Steven Griner
Organization of American States

Douglas Jones
University of Iowa

Eunsook Jung
Consultant, The Carter Center

Jennifer McCoy
The Carter Center

Adam Schmidt
IFES

Jonathan Stonestreet
Organization for Security and Cooperation in Europe, Office for Democratic Institutions and Human Rights

Thobile Thomas
Electoral Institute of Southern Africa

Rapporteurs

Kristin Garcia
The Carter Center

Ethan Watson
The Carter Center

Overview: The Carter Center was founded in 1982 by former U.S. President Jimmy Carter and his wife, Rosalynn, in partnership with Emory University, to advance peace and health worldwide. A non-governmental organization, the Center has helped to improve life for people in more than 65 countries by resolving conflicts; advancing democracy, human rights, and economic opportunity; preventing diseases; improving mental health care; and teaching farmers to increase crop production.

Accomplishments: The Center has observed 67 elections in 26 countries; helped farmers double or triple grain production in 15 African countries; worked to prevent and resolve civil and international conflicts worldwide; intervened to prevent unnecessary diseases in Latin America and Africa; and strived to diminish the stigma against mental illnesses.

Budget: $49.1 million 2005–2006 operating budget.

Donations: The Center is a 501(c)(3) charitable organization, financed by private donations from individuals, foundations, corporations, and international development assistance agencies. Contributions by U.S. citizens and companies are tax-deductible as allowed by law.

Facilities: The nondenominational Cecil B. Day Chapel and other facilities are available for weddings, corporate retreats and meetings, and other special events. For information, (404) 420-5112.

Location: In a 35-acre park, about 1.5 miles east of downtown Atlanta. The Jimmy Carter Library and Museum, which adjoins the Center, is owned and operated by the National Archives and Records Administration and is open to the public. (404) 865-7101.

Staff: 160 employees, based primarily in Atlanta.

30307

(404) 420-5100 ◆ (404) 420-5145