The Carter Center strives to relieve suffering
by advancing peace and health worldwide; it seeks
to prevent and resolve conflicts, enhance freedom and
democracy, and protect and promote human rights worldwide.

One Copenhill
453 Freedom Parkway
Atlanta, GA 30307

Contents

Carter Center Technical Team and Staff

Carter Center Technical Team

Ingo Boltz, Tecsel S.A., Carter Center E-voting Consultant, Germany

David Carroll, Director, Democracy Program, The Carter Center, United States

Avery Davis-Roberts, Program Associate, Democracy Program, The Carter Center, United States

Richard DeMillo, Dean, College of Computing, Georgia Institute of Technology, United States

Marcelo Escolar, Tecsel S.A., Carter Center E-voting Consultant, Argentina

Bill Gallery, Program Officer, Democracy International, United States

Kristin Garc'a, Assistant Program Coordinator, Democracy and Americas Programs, The Carter Center, United States

Herman Ruddijs, Business Project Manager, Department of Business Development, Sdu Uitgevers, The Netherlands

Hector Vanolli, Caracas Field Office Director, The Carter Center Venezuela, Argentina

Ethan Watson, Intern, Democracy Program, The Carter Center, United States

Carter Center Staff

Josefina Blanco, Press Officer, The Carter Center Venezuela

Glory Melendez, Accountant, The Carter Center Venezuela

Jacqueline Mosquera, Office Manager, The Carter Center Venezuela

Acknowledgements

The Carter Center would like to thank the National Electoral Council (CNE) of the Bolivarian Republic of Venezuela for inviting the Center to send a specialized, technical mission to observe the automated voting system during the Dec. 3, 2006, presidential election. We would also like to thank the government of Ireland, whose generous financial support facilitated the CenterÕs observation work for this election.

The Carter Center would like to thank the observation missions of the European Union and the Organization of American States for their close collaboration during the entire electoral period. In addition, The Carter Center recognizes the work of the domestic observer and civil society groups that played an active role in this election.

The Carter Center also thanks Richard DeMillo, Bill Gallery, and Herman Ruddijs, who were willing and able to travel to Caracas at short notice and without whom this mission would not have been

Institutional Design and Political Context of the Venezuelan Electoral Process

Observation of the electronic components of an electoral process generally includes the evaluation of the security, usability, and technical performance of the system and devices. However, observation of electronic voting should also consider the legal and institutional framework for the election, as well as the current dynamics and characteristics of the political system. These factors all have an impact on public confidence in the electoral process and affect the usability and technical performance of the system. Political polarization, for example, has an impact on the public perception of the institutions that guarantee the security of the system, which is also greatly influenced by the non-participation of opposition sectors in decision-making processes, and by any information asymmetry between political actors.[1]

Therefore, observation of the electronic components of an electoral system should be only one part of a more comprehensive effort to assess the quality of an election.

Venezuelan Electoral Authority

The current design of the Venezuelan electoral process is regulated by the Constitution of the Bolivarian Republic of Venezuela, the Organic Law of the Electoral Authority, the Organic Law of Suffrage and Political Participation,[2] the Law of Political Parties, Public Meetings and Demonstrations, and the Electoral Statute of Public Authorities. These constitutional and legal norms establish an institutional-system that creates a branch of power fully and specifically entrusted with the administration, execution, and supervision of everything related to electoral matters,[3] which is called the ÒElectoral Authority PowerÓ (Poder Electoral).[4]

Consequently, the electoral process in Venezuela falls within the exclusive jurisdiction of an autonomous state authority. To ensure its independence from the other branches of government, the constitution established the principles of organic independence, functional autonomy, and budgetary autonomy of the Electoral Authority (article 294). Thus, the Electoral Authority is in charge of preparing its own budget at the request of its chairman. The executive branch then refers it, without further modifications, to the National Assembly.

The Electoral Authority is also governed by the principles of reducing partisanship in the organisms in charge of elections, impartiality, and citizen participation, in addition to the principles of electoral decentralization, transparency, and efficiency of the vote-casting and tally processes (article 294).

1 This is a special version of the Òcapacity paradoxÓ (Hartlyn, McCoy 2006: 47), resulting from the institutional characteristics of the electoral organs, the degree of sophistication of the electronic components used, and the context of political competition. In these conditions technological uncertainty produces asymmetry, making it difficult to observe and fomenting the assumption by the political opposition that the ruling party is ÒcapableÓ of committing fraud by hidden technical means.

2 Much of this law, dating from 1997, has been amended by the 1999 Constitution of the Bolivarian Republic of Venezuela and the subsequent Organic Law of the Electoral Power.

3 In the 1999 constitution, electoral organisms were expressly recognized (article 113), whereas in the 1961 constitution, they had only legal status.

4 Similar institutional models in terms of competencies could be the Mexican Federal Electoral Institute (IFE), the Bolivian Electoral Court, the Colombian National Civil Status Registry, and the Nicaraguan Supreme Electoral Council, although none of the three mentioned cases emulate the Venezuelan electoral regime in terms of power and autonomy. In the case of Mexico, there is another specialized body, the Supreme Electoral Court of the Federation, which is not only responsible for electoral disputes, but also for the final tally and proclamation of those elected. The IFE has similar jurisdiction to the CNE with regard to electoral registration, but is not responsible for the whole documentary chain because civil registries are not subject to its administrative and hierarchical mandate. In this regard, the Bolivian Electoral Court may bear a closer resemblance to the Venezuelan Electoral Authority, though it shares some functions with the national police. In the Colombian case, full administrative responsibility for the electoral process lies with the Civil Registration Institution, though it is exempt from all jurisdictional responsibilities, legislative initiative, the final vote count, and the proclamation of elected candidates. Nicaragua also has a fourth branch of government in the Supreme Electoral Council (CSE), responsible for administering the elections, declaring final results, and resolving disputes; but in that case its decisions are unappealable to any other court or power of government.

The primary competencies of the Electoral Authority include:

¥ the ability to initiate electoral legislation;

¥ unilateral control of its budget without intervention of the executive branch;

¥ the ability to make legally binding decisions as a

¥ An ad hoc entity, the Electoral Candidacies Committee, orComitŽ de Postulaciones Electorales, is entitled to nominate three candidates on the basis of their merits.[6]

These entities propose nominees to the National Assembly. The assembly then chooses the five regular rectors of the CNE and their respective alternates by a qualified two-thirds majority vote. In general, the requirement of a super majority (two-thirds vote) in the National Assembly to elect rectors is aimed at ensuring maximum public recognition of the members of the Electoral Authority, as well as representing the body.

Current CNE

The CNE in charge of organizing the 2006 presidential elections is the first CNE designated following procedures outlined in the 1999 constitution.

In past years, the CNE members were selected via procedures different from those provided for in the constitution, thereby increasing the perception among part of the electorate of some partisanship. In 2000, in the absence of a national legislature, the Òsmall committeeÓ of the constituent assembly (Congresillo) appointed temporary CNE rectors who conducted the 2000 mega-elections. Prior to the 2004 recall referendum, the National Assembly was unable to reach a two-thirds vote to designate candidates for rectors, generating a series of petitions to the Constitutional Chamber of the Supreme Court to demand that the assembly make such designations.[7] In the end, the Supreme Court named the rectors.[8]

Design and Function of the Electronic Voting System

The Smartmatic machines are direct recording electronic (DRE) machines which capture the vote directly in an electronic memory rather than storing it on another, human-readable medium first (like optical scan systems, which read paper ballots). Due to its features, DRE machines are becoming more widely used around the world, including in Australia, Belgium, Brazil, and several U.S. states.

Two voting machine models were used in the 2006 presidential elections: the Smartmatic SAES 3000 machine and the Smartmatic SAES 3300 machine (See Figure 1).

The SAES 3000 is an older model, originally based on a lottery machine, and is manufactured by the Olivetti Company for Smartmatic. It has been in use for several years.

The SAES 3300 is a newer machine designed by Smartmatic and manufactured in Taiwan. It features several improvements over the previous model, such as accessibility aids for the disabled (e.g., audio capacity, large buttons for the blind). However, in the 2006 Venezuelan elections, none of the differentiating features of the 3300 model were used because the software to incorporate them was not ready in time for the elections.[15] Therefore, the 3300 model ran the same voting software[16] as the 3000 model with the extra features of the machine unused. Consequently, this report generally will not distinguish between the two models.

Both machines run Windows XP Embedded as their operating system and voting software specifically developed for the Venezuelan elections, written in the programming language C# using the Microsoft .NET framework.

Smartmatic SAES 3000

Smartmatic SAES 3300

Figure 1: Smartmatic SAES 3000 and SAES 3300 voting machines

Hardware

The SAES 3000 and SAES 3300 models share the following key hardware features:

- color touch screen (the 3300 screen is slightly larger)
- integrated thermal printer with paper cutter
- internal disk on memory (no hard drive)
- various communication and periphery ports (an Ethernet port and a modem)
- included USB memory stick with separate port
- physical lock to prevent opening of the machine

Peripheral Components

Both models work in conjunction with the same set of peripherals:

- Remote machine activation button connected by cable to one of the machineÕs PS/2 ports (see Figure 2).

15 Source: Interview with CNE technical staff.

16 Some operating system details such as device drivers may have varied between the two models because the hardware is not exactly the same in both machines.

Figure 2: Remote activation button

¥ Touch pad containing ballot options (to be connected by cable to one of the voting machineÕs PS/2 ports). The ballot options are printed on a paper ballot that is placed over the touch padÕs touch-sensitive buttons. The paper ballot indicates the spot the voter needs to press to hit the underlying button. In the 2006 presidential elections, all ballot options were arranged on one pad. In previous elections, several pads, connected serially to one another with the last connected to the voting machine, were used (see Figure 3).

Functional Description of the System on Election Day

The following is a description of the part of the voting process that concerns the operation of the DRE voting machine. This includes an account of the opening of the polling center, voting itself, and the closing of the polling center.

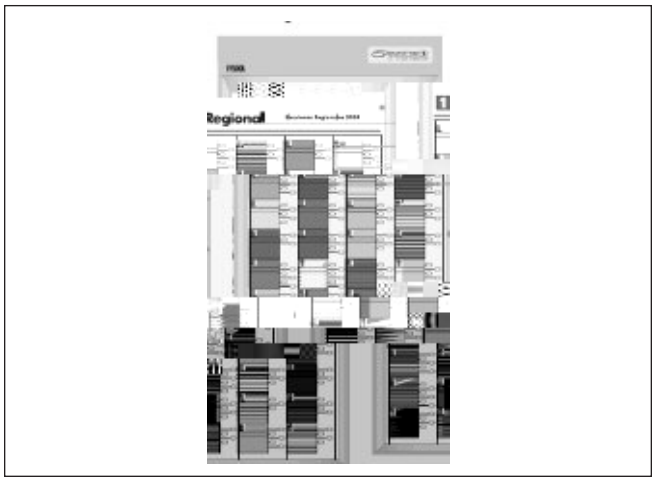


Figure 3: Touch pad containing ballot options

Opening of the Polling Station on Election Day

To open the polling station, CNE regulations required the following steps:

¥ The operator verifies that the physical conditions to operate the voting machine are met (e.g., electric power is available, vision shields for privacy are set up).

¥ The machine operator enters a password unique to each machine using the touch screen to unblock the voting machine and enter the operator menu.[17]

¥ The machine operator accesses the technical menu and performs system diagnostics to verify that all components work correctly. A diagnostic report is printed. In case of failure, contingency procedures are followed.

¥ The machine operator starts the voting process with the printout of two zero tape records.

¥ The first voter may start voting.

During Voting on Election Day

During the voting stage, the following steps were taken:

Access authorization

After the voter has identified himself or herself, the voting table president presses the remote machine activation button located on his or her desk. This unlocks the voting machine for three minutes. If the voter has not cast a vote within three minutes, the machine automatically locks. The voting table president then needs to press the remote machine activation button again to allow another three minutes of voting time. Only two three-minute periods are permitted for each voter. After that, the machine will not be unlocked again.[18]

17 This menu controls functions hidden from the voter such as diagnostics, poll opening and closing, and transmission.

18 This is not a technical restriction of the voting machine but rather a policy imposed by the CNE.

- The machine operator connects the machine to a means of communication and transmits results to the tally server. If transmission from a polling station fails, or if transmission is impossible from that polling station because of a lack of either fixed or mobile connectivity, the memory stick containing one of the two copies of the full set of votes is removed and transported to the nearest contingency transmission center from where its results are then transmitted to the tally server.
- The machine operator prints out the chorizo a reprinted nonsequential backup copy of paper voting slips.[19] These printouts look exactly the same as the ones verified by the voters and placed in the ballot boxes and are therefore essentially a second version of the precinct tally result reports in the form of paper ballots. According to the electoral authorities, the main goal of the chorizo is to help polling station authorities to identify any missing

or her choice and deposit it in the ballot box. The human handling of the paper slips allowed for human errors such as voters accidentally or intentionally taking the slip home with them. Because of this circumstance, the CNE should consider implementing further practices to avoid the physical manipulation of the paper slip. A commonly accepted alternative practice is for the paper slip to be displayed to the voter behind glass without the voter handling it.[23]

Moreover, Carter Center observers noted that there are no procedures in place for cases in which the voter alleges that the paper slip does not match the vote that was displayed on screen. This circumstance undermines the purpose of a voter verified paper trail. The voter, upon perceiving a discrepancy between screen and printout, should have the chance to cancel his or her vote Ñ both the electronic vote and the paper vote Ñ and vote again. In such circumstances, the electronic vote should be deleted and the paper slip invalidated, either through physical destruction or overprinting with a ÒcancelledÓ notice.[24] In the Venezuelan design, a voter who alleges such discrepancy cannot cancel his or her vote.

During election day, a member of the Carter Center mission observed a female middle-aged voter who claimed that the paper didnÕt match the vote she had cast on screen. The polling station authorities asked her to deposit the paper regardless, which she refused to do. In the end, she ripped the paper in pieces and stuffed it in the ballot box, leaving in protest.

Another concern is the fact that the paper slip, which is meant to allow the voter to confirm that the machine correctly captured his or her vote, did not contain images of the candidate. An illiterate voter, while being able to cast his or her vote on the screen guided by the candidate image and the party symbols, could not confirm that vote on the paper slip, because it contains neither element.

Finally, the time limit imposed on the voter by the voting machine may raise a serious conflict between security requirements and the right to vote. In its current configuration, the machine allows only three minutes for the voting process, with a single extension of three additional minutes before locking. This measure is meant to prevent unauthorized access should a voting machine be left unattended after having been unlocked by the table president. However, in practice, this circumstance also limits the number of vote attempts that the voter has the right to make.

Summary of Recommendations

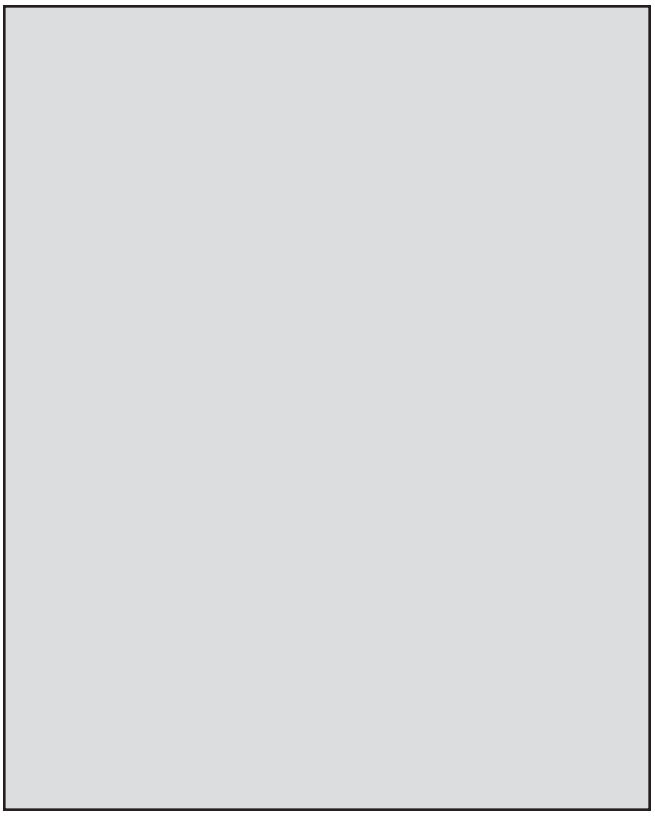
- Remove the paradigm break of the user interface process for the null vote. The touch pad should contain a separate button for Ònull voteÓ and that option should be displayed and confirmed on the touch screen just as with regular votes.
- Change the paper trail design to minimize manual handling of the vote slips to prevent unintentional removal of the paper ballot slips from the polling station.
- Allow voters the opportunity to cancel their votes if the receipt does not accurately reflect their choices.
- Include candidate photos and party symbols on the paper slip to allow illiterate voters to confirm their votes unassisted.
- Reconsider the Òtwo times, three minutesÓ policy for voters. Voters should not lose the right to vote because they have difficulty navigating the technical system in use.

23 Examples of such designs included the newer Diebold AccuVote TSX voting machine with AccuView printer, the Diebold/Procomp machine with printer that was used in Brazil, and the prototypes REV and LO used during the electronic voting trial in Buenos Aires 2005. See Calvo, Escolar, Pomares (2007), Gobierno Ciudad Autonoma de Buenos Aires (2005).

24 Diebold AccuVote TSX and Buenos Aires prototypes, ibid.

Paper Receipt Slip Security

The paper receipt slips recording the voter-verified vote contain a significant number of anti-counterfeit measures. For instance, the slips are watermarked and printed on special paper identified with the logos of



Results Transmission

to the voting machine using a serial cable and then performing dial-up, connection, and transmission in a similar way to the fixed line procedure.

Satellite telephone line. This transmission method was only used in some CTCs in remote regions where no other transmission was possible. CTCs in most urban areas used fixed lines.

The network infrastructure was specifically provided for this electoral system by CANTV, the

Transmission Security Measures

There are several layers of security used to safeguard results transmission.

¥ Dedicated infrastructure Ñ (partly virtual) private network. Only telephone lines (both fixed and mobile) listed on a white list could dial a previously established number and connect into the regional RAS to gain access to the private network. The white list contained details of the fixed phone lines installed in polling centers and CTCs,[48] as well as the specially-issued mobile phones of the machine operators and technicians. The fixed phone lines and the mobile phones could neither send nor receive calls from the public telephone system.

The day before election day the white list was purged of any Ògrey candidates,Ó such as cell phones of machine operators who had not been showing up for work.[49] Similarly, for satellite connections, a list of approved Òsatellites modemsÓ was created. Only accepted modems could communicate into the network.

Between the regional RAS servers and the central CNE servers (called ÒCNT 1Ó and ÒCNT 2Ó) the results data traveled over a virtual private network (secure tunnels using IPsec). The same IPSec tunnel architecture is used to connect:

Ð The CNEÕs CNT1 with its contingency CNT2

Ð Internally the CNE application servers (REIS listener and consultation servers, see below) with the database servers

Ð The regional election authorities (juntas regionales) with the CNT (which were used as regional CTCs)

¥ The database servers only allow queries from the CNE application servers (restriction based in IP tied to MAC address).

¥ RADIUS/AAA authentication of all dial-up and mobile CDMA connections. All voting machines whose connection attempts were permitted because their phone lines were white-listed needed to additionally identify themselves with a username/password scheme against a RADIUS server.

¥ Encrypted communication (SSL v3/TLSv1) with two-way authentication using a certification created by the CNE and Smartmatic on the day of the elections and digitally signed by the CNE/Smartmatic certificate authority. The packet content was also digitally signed. This scheme was used for the transmission between the voting machines and the CNT, and for the web interface used to live-query the results database during election day.

¥ Firewall protection of CNT1 & 2 (with SPI/IDS/IPS capacity).

¥ Centralized location of CNE physical computing resources with restricted physical access and restricted access to administration of servers, switches, firewalls etc. (access codes shared between vendor and CNE).

> For the December 2006 elections, several procedural security measures were implemented, most of which were agreed upon with opposition sectors during the months before the elections.

Additional Measures

Beyond that, for the December 2006 elections, several procedural security measures were implemented, most of which were agreed upon with opposition sectors

48 We could not clarify whether these fixed phone lines were specifically installed by CANTV for the elections or if existing phone lines were used. Dedicated phone lines are more secure.

49 According to information communicated verbally by CNE officers, an audit was performed with the purpose of cleaning the Òwhite listÓ a day before the election. The audit was specifically designed for this purpose.

Given its implications, this circumstance is in itself a weakness of the usability of the system. Thus, the CNE should consider implementing viable solutions to address this problem. One such alternative could be to forbid changes to candidate alliances once the paper voting ballot is printed. Even if short-notice changes to candidate alliances could be implemented in the screen display, the discrepancy between ballot touch-pad and screen would create unacceptable confusion.[51]

Since endorsement changes cannot be managed locally, they were managed centrally in the PEM. Changes of endorsement were entered into the PEM via a Web interface[52] by regional electoral authorities and needed to be certified by the National Electoral Board (JNE) before becoming active. If approved, the PEM module made sure that votes for the respective party are counted towards the newly endorsed candidate instead of the old one. Having technical details of this certification process and the details of the security policies that regulate access to this sensitive module would allow a more thorough analysis of the security of the PEM system.

REIS Listener

The REIS listener is an application server which received the vote file transmissions from both the voting machines and the regional electoral authorities (which transcribed manual polling placesÕ results and transmitted them to the CNE).

The REIS listener had the following functions:

- ¥ To verify the client certification that each voting machine presents
- ¥ To receive the transmitted packages (containing the vote results)
- ¥ To validate packet integrity
- ¥ To connect to the database server and record the results in the database.

The REIS listener only receives, verifives,(Give727.beult75.8037 gs q 00001 TD 0.ltssho3spdrrti30<eT79.i4 TD

central tally system itself remains hard to evaluate. It appears that the central tally system would benefit from additional layers of security that would protect it from potential internal malicious exploitation in a future election. One such measure might include the use of an independent, industry-recognized third party certificate authority to issue the certifications securing the communication between voting machines and the tally center

Summary of Recommendations

- ¥ Consider using an independent certificate authority to issue the certifications securing the communications between the voting machines and the tally. This additional security measure would help to protect the central tally system from potential attacks.
- ¥ Increase the role of political parties and observers in the audit process by allowing formal election day observation of the central tally system, including greater access to observe such critical tools as the PEM. This would increase transparency and help to establish check and balance security mechanisms.
- ¥ Last-minute changes of political parties/ candidates alliances should not be allowed. This would prevent the introduction of changes in the PEM that are not reflected on the ballot.

Audit Schemes

it is likely that6a2rors wiw0 /F11e4ie overlooks304.857.29fm.

During this audit, the sample of 164 voting machines (0.5 percent of the total of 32,331 produced) previously selected during the production audits were tested.

The main objectives of the pre-dispatch audit were to simulate the voting process that would take place on Dec. 3, in order to prove that the machines worked as intended and that the electronic voting results recorded in the machines and in the central tallying system were the same as those physically recorded on the paper receipts printed by the voting machines (which would be visually verified by the voter before depositing it in the ballot box). A further objective was to prove that the version of the software installed on the voting machines was the exact same version as that audited and approved by the political party representatives during the previous source code audits.

Description of Procedure and Observations[66]

The pre-dispatch audit took place in the same place where the machine production audit had been previously executed.[67] Voting machine operators, support technicians and CNE staff, party representatives and observers participated in the audit.[68]

The pallets with the sample machines to be audited had already been identified and set aside the previous day (observed by The Carter Center mission) to speed-up the process of unpacking. In order to begin the rehearsal, CNE staff and political party representatives proceeded to remove the seals from the pallets, open the boxes and place the voting machines on a number of tables, where the operators would enter votes, observed by political party representatives.

Because there were only 48 tables available for this exercise (presumably due both to restrictions on the physical space and the number of available machine operators), not all of the 164 voting machines could be set up at the same time. Consequently, the rehearsal of the voting process k8pF11 1 Tf 11l, at4.6625 356.6787 Tm 0 0 0cTD .301.2e for thisbars2 TD (machi

Becafor this5.52261.edesaTD (os2 ke exact)Tjical labded inouj .6787bars2 TD (maranon wrsin [3iaryintral)Tjodcha

164 voting machines (or 3 percent) were reported to have malfunctioned and therefore had to be replaced with contingency machines.

On a small sub-set of machines (six out of the total of 164, or 3.6 percent) a hash verification process was performed in order to verify that the installed software matched the version audited, approved and digitally signed by the party representatives. For this purpose, an external keyboard was attached to the select ed machines, and from a special memory stick, a Linux operating system was booted, which included the CNEÕs hash verification software, and a file containing the hashes as recorded during the source code audits. This software was run and generated hashes of the archives which comprised the voting software installed on the machine. These hashes were-com

J Te037 l365 l 297.mNmachin9 3061 le c2385.w1Olt aaystem was booted, (of)nThissmalus[(J Te03)nThis puofor 3
71j T*ET59.8582 3098583 309.902 759.8583 v f Q Q Q /68.0.7 q BT /F11 1 Tf 11 0 0 11 54 2385ol memors pere

- A 50-vote limit was established with the system forward procedure, the fact that the number of votes entered was capped at 50 for most of the machines represents a significant difference from voting day conditions, where up to 600 votes may be cast. A malignant code might activate only after a larger number of votes have been cast, effectively bypassing the test situation undetected. Party representatives tried to counter such a potential threat by trying to input a large number of votes during the one hour vote casting period.
- Only one hour of vote entry activity and resulting high voting speed. A malignant code that is triggered by voting speed might not be caught by this test. Voting on election day would be much slower than during the test, and the code might only activate if voting did not exceed a certain frequency effectively bypassing the test situation without detection.

> While generally without major incident, The Carter Center mission observers did note some confusion about appropriate chain-of-custody procedures.

Because of these shortcomings, the pre-dispatch audit, while perhaps useful as another system test before elections and a means of building public confidence, was of limited value as proof of system integrity[74]

Election Dry-Run

The election dry-run, which took place on Friday, December 1, was not part of the technical audit scheme. Its objective was to verify the integrity of the voting machines and their components (and replace any lost or damaged parts, if so required) in order to prevent problems from occurring on election day. Therefore, during this test, the delivery and reception of the voting machines in the polling places, trial setup of the machines (to check for errors and missing components) and a rehearsal of the constitution of voting tables and table authorities were observed. The Carter Center mission observed a polling place chosen by the CNE,[75] and several other polling places selected randomly by Carter Center observers themselves.

While generally without major incident, The Carter Center mission observers did note some confusion about appropriate chain-of-custody procedures. In addition, among rehearsal participants, there appeared to be a heavy reliance on the expertise and authority of machine operators rather than on polling officials. In addition, The Carter Center mission noted that military personnel played an active role in the rehearsal process. This seemed to be especially pronounced in the CNE determined polling place.

In the polling center picked by the CNE, the tamper seals on all of the machine boxes were broken. Upon discovery of this fact, the machine operators stated that they had needed to open to boxes during the delivery handover the previous day, and that that was part of procedure. The Carter Center mission observed that official procedures require that the boxes remain unopened and sealed when received (although this is contradicted by the operator manual which demands an Òinventory of all machine parts,Ó without making clear that this has to take place in the presence of the table authorities and witnesses during the dry-run and not before.)

Responding to the concerns of the table authorities, the operators stated that an invitation had been sent to them asking the mentioned authorities to be present the previous day for the opening of the

74 For a comparable criticism of the Brazilian ÒParallelÓ election day procedures, see Rezende (2004).

75 Colegio Nuestra Senora de la Consolaci—n, in Caracas

In addition to the observation of audits set up for election day, during this day The Carter Center mission also partly observed the procedures performed at the CANTV Network Control Center on election day. However, the activities undertaken in the CNE tally center could not be observed due to a CNE decision establishing a limit to the number of international observers in the premises.

Tally Center

Two observers (one from the EU and one from the OAS) were present in the tally center in the CNE headquarters for several hours on election day, observing CNE and vendor staff as they monitored the system, incoming voting data, IDS etc. Since the CNE decided to only allow two international observers to be present in the tally center, The Carter Center mission could not be present. Nonetheless, observers who were present in the tally center shared their observations with The Carter Center. According to their report, no irregular activity was observed in the center.

CANTV Network Control Center

A Carter Center observer was present in the CANTV network control center, observing for several hours the network traffic caused by the system. The observation was prematurely terminated when the observer was denied re-entry by CNE authorities after taking a break. The details of the observation until that point, including the concrete traffic numbers observed, plus graphs and schemes, are available in the appendices. The summarized results are the following:

- Until approximately 6:00 p.m. no unexpected traffic was observed.
- Shortly before the abrupt end of the observation, a leveling off of the number of voting machines transmitting was observed.

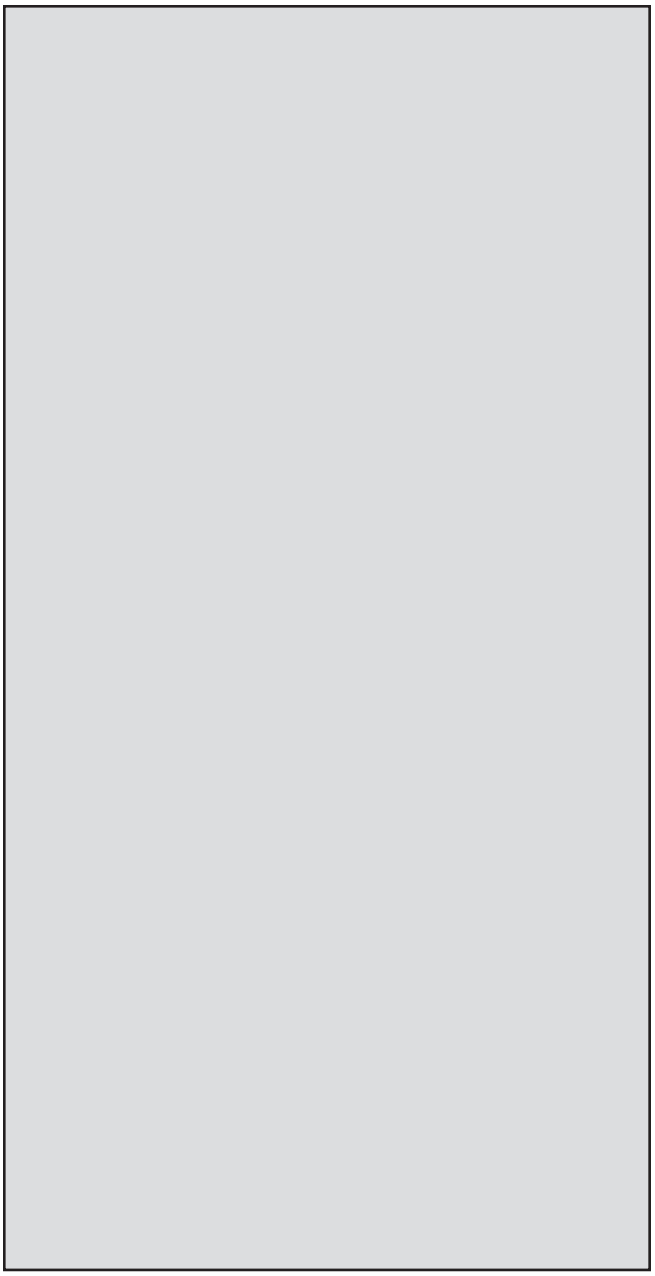
This sudden and unexpected change in network traffic is consistent with reports from polling stations across the country that in many polling stations table authorities were asked by the CNE or Plan Repœblica to delay the closing of voting tables (and hence transmission) in order to allow more voters to vote.

Postelection Audits

At approximately noon on election day, a random selection of one percent of all polling centers was performed in the CNE headquarters[77] in the presence of party representatives and observers. Machines from these selected polling centers would later be audited in the post-election audit. The selection was made by

77 Which made 106 centers in total (or about 0.5 percent of the total universe of voting machines).

the audit teams looked for missing original paper slips amongst the backups, and when found, used these instead of the missing original. If there were still discrepancies after the initial recount, more recounts were ordered. The teams recounted until the numbers matched the precinct tally record printouts, usually on the grounds that human error was most probable. Procedures specified that, after a certain number of unsuccessful recounts, the dis



Conclusions and Recommendations

documents, could be handled jointly with political party representatives[88]. In addition, the chain-of-custody procedures should be widely publicized amongst all stakeholders in the electoral process, and chain-of-custody personnel lists made public so that any violation of procedure can be easily observed by any actor involved, so that the Òmany eyesÓ principle may be achieved.

a4n9ue mani57473907 i2-ation ma20s1dn1p..9383 309.902 75909.94onsiy2T81.0902 2he b9y 3[tem. t b829.9

To further increase public confidence in the electoral process, The Carter Center also suggests that the CNE consider establishing an independent certificate authority to certify both the system and the system documentation, and to verify that the actual system corresponds exactly to the published CNE specifications. Eventually, this certification body could certify the totality of the electronic voting system in regard to its security and make recommendations for its improvement.[86]

An increased role of the political parties, especially the opposition, in the process would also increase public confidence in the CNE and in the electronic voting system. This may include additional audit measures that can be independently performed by the opposition, but are well defined parts of the regulatory framework. For example:

- Opposition auditors could be allowed access to voting machines of their choice during the pre-election audits in order to verify the hashes of installed software.
- If witnesses report irregularities at polling stations, opposition experts could be guaranteed the right to inspect the machines retrieved from these polling stations for irregularities.
- Opposition auditors could be allowed to observe the tallying center. This would imply greater access to real-time result monitoring tools and to critical tools such as the party endorsement manager (PEM).

86 In an interview, opposition auditors stated that the creation of such an independent, multi-party expert organism to develop the audit schemes and certify the technology had been proposed but thus far rejected by the CNE. Examples of other models include the Commission on Electronic Voting in the Republic of Ireland, which has a mandate to provide an independent evaluation of the performance of the electronic voting system, particularly with regard to secrecy and accuracy of the technologies. Composed of county clerks, and the chairmen of the Science Foundation Ireland and the Information Society Commission, this body does not certify electronic voting technology itself, but has the ability to review certification tests that have taken place, and to commission new tests. (For more information, please visit http://www.cevie/index.htm.) The Center for Election Systems in the state of Georgia in the U.S. is housed at a university. Staffed by academics and technical professionals, the center conducts independent acceptance testing and conducts training for poll workers and machine operators. (For more information please visit www.elections.kennesaw.edu.) The Physikalisch Technische Bundesanstalt (PTB) in Germany is an independent laboratory that functions under the auspices of the Federal Ministry of Economics and Technology. PTB provides independent verification of internet and electronic voting solutions and is developing guidelines for the development and testing of online voting systems. (For more information please visit http://www.ptb.de/index_en.html.)

References

ACT (2001) The 2001 ACT Legislative Assembly Election Electronic Voting and Counting System Review. Election Review Computer Voting. http://www.elections.act.gov.au/adobe/.

Because of its relatively limited size and duration, The Carter Center technical mission did not aim to obtain statistically relevant observation results. Rather, it tried to collect examples and anecdotes from which rough conclusions could be drawn regarding the influence of our factors on the election process, selected by the Carter Center team. For the same reason, Carter Center teams were encouraged to observe the electoral process as a whole, focusing on one to three polling stations during the day and capturing the complete process at one of them. Rather than emphasizing breadth of observation, the mission aimed for depth.

The Carter Center observer teams were sent to polling stations on the basis of the following variables: expected degree of participation; expected degree of polarization; and transmission method used.

Variable 1: Expected Degree of Participation

The objective of observing this factor was to judge the performance of the voting system in three scenarios:

¥ High usage stress (high participation, many voters in rapid sequence)

¥ Low usage stress (low participation, few voters)

¥ Normal usage (medium participation)

This variable had potential impact on the voting process throughout the entire voting day

Variable 2: Expected Degree of Polarization

This variable is related to the percentage of ruling-party voters vs. opposition supporters (data base from 2004 referendum). This factor translates into the following scenarios:

¥ Low degree of vigilance regarding the use of technology (under large ruling-party majority)

¥ High degree of vigilance regarding the use of technology (under large opposition majority)

¥ Reciprocal control and vigilance (through strong competition between the ruling-party and the opposition)

This variable has potential impact on the opening and closing procedures, as well as the general voting process during the day.

Variable 3: Transmission Method Used

The transmission methods used on election day were taken into account in this variable:

¥ Transmission by fixed telephone line

¥ Transmission by mobile phone

¥ Transmission from contingency transmission articiee of

Since geographic location bears little influence on our chosen factors, polling stations nearby were selected (Caracas Metropolitan Area and State of Miranda). In order to amplify the scope of anecdotal evidence collected, a number of backup polling stations near the principal ones were picked. During periods of little activity at the principal stations, the observer teams could roam to these additional ones. Observers were required to be present at the principal center during poll opening and closing. This way, the observations on voter interactions with the voting machine user interface would be maximized, and observers would be able to assess machine usability in general.

Anecdotal results of the observation have been used throughout the final report of the mission to illustrate various aspects of the voting system. In general, Carter Center observers found increased tension in those polling places where support for political parties was roughly equal, as was to be expected. ÒRuling partyÓ polling stations generally displayed a low level of scrutiny and a greater number of technical doubts, however, problems with the user interface (UI) were more common. Opposition strongholds generally displayed smooth operations and a high level of technical understanding with fewer problems with the UI.

Appendix B
The Audits in Detail

This section provides a detailed account of the audits conducted for the 2006 presidential elections.

Voting Machine Source Code Audits

ÒGenKeyAndProtect,Ó which was compiled in the presence of the parties.

¥ A series of hash values was created (Md5, SHA-I, SHA-256), both of the compiled and protected applications and the source code files. All these hash values were stored in a text file called ÒPlantilla_Hashes_Binarios_y_Fuentes.txtÓ of which again three hash values were generated (Md5, SHA-I, SHA-256); those values were recorded in the minutes.

¥ A visual code review was performed of the parts of the source code covering the encryption scheme used in the voting machine, including management of contingency passwords.

Notes and Observations:

It is not clear whether the software compiled in this session includes tally center software. From the list of applications compiled, this does not seem to be the case. Apparently, this code review was done by showing the source code to the auditors on screen and going through the lines of source code one by one. Source code could not be taken by political parties and/or analyzed using the political parties representativesÕ own tools.

Oct. 18:

According to the official minutes the following happened:

After verifying the respective hash values, it was found that the OS image installed on the PC used for the audit Òdid not have network card drivers,Ó those drivers were installed, a new operating system image (including the drivers) created and new hash values for that image generated and recorded.

Notes and Observations:

It is not clear why network card drivers needed to be added. According to specifications, the voting machine does not use its built-in Ethernet network card to communicate during election day. Following security procedures, the card should have been disabled in the system registry since the machine does not need it and its active presence presents an unnecessary security risk. Consequently it would only make sense that the OS image intended for later installation on the voting machines would not contain these drivers.

Oct. 19:

According to the official minutes the following happened:

Revision of the voting process and revision of the vote transmission process.

Notes and Observations:

No further detail was included in the official minutes.

Oct. 20:

According to the official minutes the following happened:

Revision of the voting process, revision of the precinct count report transmission process, precinct count report, and evaluation of test tools.

Notes and Observations:

No further detail was included in the official minutes.

Oct. 23:

According to the official minutes the following happened:

Revision of the voting machine environment handler; revision of mechanism that prevents vote sequence reconstruction (using NTFS explorer); trial installation of a 3300 machine; and trial voting, generation of tally count report, and comparison with votes cast.

Notes and Observations:

No further detail was included in the official minutes.

Oct. 24:

¥ Hashes were generated of the encrypted sample files. Those hashes were compared to their corresponding hashes from a list of all hashes of all encrypted configuration files, which was previously provided by the CNE.

¥ A list of non-confidential, electoral-only information was extracted from the non-encrypted sample files and given to the party representatives.

¥ The previously mentioned list of all hashes of all encrypted configuration files ÒwasÓ verified in all the burn stations.[90]

Central T ally System Source Code Audits

According to the official minutes, source code audits of the central tally system took place between Oct. 25 and Nov. 30. Carter Center observers were not personally present during any of these audits. While most audits took place prior to the arrival of Carter Center observers, two audits did take place after the arrival of The Carter Center. Given that no notice was given of these audits, it was not possible to have access to them.

Oct. 25:

According to the official minutes, a kick-off information session took place, where the functionalities of the central tally system were introduced. An initial timeline for the following source code audit sessions was determined.

Oct. 26:

According to the official minutes the following happened:

¥ Revision of the reception module (REIS listener)

¥ Initial inspection of reception module source code

¥ Inspection of database tables used by the reception module

¥ Generation of a hash of the source code of the ÒentireÓ application

¥ Creation of detailed inspection schedule for modules

Oct. 27:

According to the official minutes the following happened:

¥ Verification of the hash value generated at end of audit on Oct. 26 to verify no code had been modified

¥ Continued revision of the reception module (REIS listener)

¥ Revision of complete functional flow taking place once a transmission is received from a voting machine

¥ Revision of the process of storing voting information in the central database, verifying the validation mechanisms

Oct. 30:

According the official minutes[91] a detailed review of the business logic of the REIS listener took place, resulting in a table of reception cases. Their resulting handling by the REIS listener, plus the according status codes were saved in the database for the events.[92]

Oct. 31:

According to the official minutes the following happened:

¥ Revision of database scheme

¥ Further revision of the Web-based result consultation module

¥ Performance of transmission tests

¥ Input of records from manual votes into the system, simulating that part of the process applicable to the few non-automated voting tables to be used

Nov. 3:

According to the official minutes the following happened:

90 Presumably memory stick copy centers

91 The proceedings of Oct. 30 are noted in the minutes of Oct. 31, making this document the combined register of both daysÕ proceedings.

92 The table is too long to be represented here.

9. The auditors entered the production facility itself as a group. The auditor office is located in an annex of the building. At the entrance, they were checked with a metal detector by the Plan Repœblica military personnel guarding the facility. They were not allowed to come in with cell phones, memory sticks, or other metal objects inside.

10. The auditors were led to a part of the plant where the machines were loaded onto trucks for shipping. There, a pallet with the two boxes containing the selected machines, plus two boxes for the machinesÕ (separate) ballot selector unit, in total four boxes, waited for them. These boxes had supposedly been retrieved from the assembly hall area by plant staff and put there for the audit.

11. The auditors verified that the information sticker glued to the boxes matched the chosen numbers. They did not open the boxes; the boxes had unbroken CNE tape seals.

12. Upon finding that the documentation on the boxes matched the chosen numbers, the auditors

at random could be switched for others during the unsupervised Òsearching and preparing of the sample machinesÓ by the plant staff, the answer was that because the software of each machine was unique (because it contained information about its unique location) this would be ineffective. During the pre-dispatch audit, any discrepancy between the unique geo-coded ID recorded in the minutes (ID1) and the ID1 of the machine would be noticed.

Whether this argument is valid depends, however, on the speed with which a clone can be created. If it is possible, upon learning the chosen numbers, to take blank machines and program them with the same geographic information according to the machines randomly chosen by the auditors, place them into boxes labeled like the correct machines, and present these for audit, in the 15 to 20 minutes the auditors waited for the machines to be retrieved and presented for sealing, the auditors could have been presented with replacement machines without knowing it. During the later pre-dispatch audit of these sample machines, the discrepancy would not be noted because the geographic information programmed into each machine matches the one recorded in the minutes. Obviously, if a swap would take place, auditing a specially prepared sample machine, instead of a randomly chosen machine of the type that is shipped to all the country, would make the pre-dispatch audit meaningless.

The pallets with the boxes were not sealed completely because the underside was left unsealed. If speed issues (or that fact that the swapping would have to be done in the middle of a production run with all the personnel on the production floor present in the vicinity) would prevent a Òhot swappingÓ operation, the question remains whether the applied seals are effective. Because the signed seals are not directly attached to the boxes (but rather to the pallet), a machine would

CANTV Network
Traffic Control Center

Date of Observation	Dec. 12, 2006
Carter Center Observer	Ingo Boltz
Place of Observation	CANTV MiniCore network traffic control center for CNE virtual private network
Objective of Observation	Observe network traffic in the CNEÕs virtual private network, (provided by CANTV) as it developed on election day. Watch for traffic activity before 4:00 p.m. (time when voting machines are scheduled to start transmission to central tally server) and observe potential irregular network activity thereafter.
Organizations present during Observation	Comando Miranda CANTV employees

Description of Observations:

Observation began after we gained access to the MiniCore area at about 4:15 p.m. At this time, little traffic was visible. There were attempts of voting machines trying to connect but the CNE router was not assigning IP addresses to the machines. (See Figures B.2 and B.3.)

¥ At about 16:30 (4:30 p.m.), CNE began assigning IP addresses and accepting communications, begin-

The information gathered by answering these questions should create a comprehensive picture of the voting system in use and thus

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 systems? Is 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

Voter Verified Paper Trails (VVPT)

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?

Pre-election Testing

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. c. 556f. f. otentiote suspicious behaviorvotes

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.

Electronic Poll Books and Voter Identification

104. If electronic poll books are used, who is responsible for creating the database that is used and who has

Accessibility

121. Are ballots available in minority languages?

122. Do voters in the following circumstances use electronic voting technologies to cast their ballots? (Circle all that apply)

   a. Confined to a hospital
   b. Confined to home
   c. In prison
   d. Outside electoral district on election day

123. Does this equipment undergo the same testing as the equipment deployed to polling places?

124. Is provision made for voters who are disabled or illiterate?

125. If the machines produce a voter verified paper trail, does the paper ballot appear in such a format that it is clear to illiterate or disabled voters that their vote has been correctly cast?

Election Day Procedures

126. Please describe the intricacies of election day procedures as specified by the election law or the rules and regulations of the electoral management body, including the following:

   a. Poll opening and setup of all equipment (including production of zero tape, ensuring that all items are present and accounted for)
   b. Connectivity of equipment during the course of the day (including when, why, and how long the machines are connected to a network and what security and authentication measures are in place)
   c. Voting process
   d. Storage of spare equipment
   e. Poll closing procedures

b. Replacement equipment is available in the event of malfunctions. If so, is this replacement equipment the same model as the technology it replaces? Is it deployed from a central location or kept at each polling place? (Please describe)

c. Substitute technology is subject to the same testing and evaluation procedures as equipment originally deployed to polling places.

d. Chain-of-custody procedures are in place for equipment taken out of service during an election. If so, is this chain of custody documented and are any of these documents available to the public?

e. A process for documenting malfunctions, failures, or errors is in place.

f. A process for obtaining election day performance records (e.g., errors and malfunctions) of specific equipment is in place.

g. Contingency plans and procedures for partial or total power outage are in place.

130. What contingency planning training is in place for polling officials? Please describe and attach any pertinent information.

131. How do polling places and central offices communicate in case of emergencies, such as power outages, telecommunications failure, and so forth?

Ballot Counting and Recount and Complaint Procedures

132. How are ballots counted at the end of the election? Please describe.

133. Are results printed and publicized prior to their transmission to the central tabulation system?

134. Are paper ballots counted at the end of election day? If so, is the tally compared to the electronic result tally produced by the voting machine?

135. Are paper ballots from all machines counted, or is this process conducted on a statistical sample? If so, what sampling method is used?

136. What procedures are in place if there is a discrepancy between the paper ballot count and the electronic tally?

137. What triggers a recount?

a. Voter application

b. Candidate application

c. Narrow margin of victory

d. Automatic random recount

e. None of the above

f. Other (please describe)

138. Can a recount be requested regardless of the margin of victory?

Polling Station No.: _____

Team No.:_____ Time of Arrival: _____

City/District: _____ Time of Departure: _____

Province:_____ Date: _____

1. What technology is used in this polling station?

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

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

_____

_____

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

_____

_____

6. Who delivered the equipment to the polling station?

_____

_____

7. Was this chain of custody documented? Yes No

8. tsh c7es, w demn otn othe nucumentedion?_____

_____

Poll Opening Ñ Electronic Poll Book Observation

2. Which communication method is being used in this polling station?
   a. Fixed-line telephone l
   b. Cellular telephone l
   c. Satellite telephone l
   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?

_____

_____

7. Who delivered the equipment to the polling station?

_____

_____

8. Was this chain of custody documented? Yes No

9. If yes, who main9e3 mai150210 T68.0441737T /Fe -2.0et1.0e8 601 0 0 0 12k 0.0253on, bu3 .11284transmiss

Appendix G: Poll Closing