THE
CARTER CENTER

# Observing the 2006 Presidential Elections in Venezuela

## Final Report of the Technical Mission

*Waging Peace. Fighting Disease. Building Hope.*

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.

# Observing the 2006 Presidential Elections in Venezuela

## Final Report of the Technical Mission

THE
CARTER CENTER

One Copenhill
453 Freedom Parkway
Atlanta, GA 30307
(404) 420-5188
Fax (404) 420-5196
www.cartercenter.org

November 2007

# 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 García**, 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

# Terms and Abbreviations

| | |
|---|---|
| AAA | Authentication, Authorization and Accounting |
| AES 256bit | The Advanced Encryption Standard in cryptography, with key length of 256 bits |
| AFIS | Automated Fingerprint Identification System |
| BIOS | Basic Input/Output System |
| CA | Certificate Authority |
| CANTV | *Compañía Anónima Nacional de Teléfonos de Venezuela* |
| CDMA | Code-Division Multiple Access, a digital cellular technology |
| CNE | *Consejo Nacional Electoral* |
| CRCE | Civil and Electoral Registration Committee |
| CPU | Central Processing Unit |
| CTC | Contingency Transmission Center |
| DLL | Dynamic Line Library |
| DOM | Disk On Module, an alternative to traditional computer hard disks |
| DRE | Direct Recording Electronic machines |
| EA | Electoral Authority |
| eVote | Electronic Vote |
| IDS | Intrusion-Detection System |
| IP address | Internet Protocol address; an identifier for a computer or device on a TCP/IP network |
| IPS | Intrusion-Prevention System |
| IPSec | IP Security, a set of protocols developed by the IETF to support secure exchange of packets at the IP layer |
| JNE | National Electoral Board (*Junta Nacional Electoral)* |
| IT | Information Technology |
| ICTs | Information and Communication Technologies |
| MAC address | Media Access Control address of a computer networking device |
| MD-5, SHA-I, SHA-256 | Hash algorithms |
| Memory Stick | Portable flash memory, usually connected to the USB port of a computer |
| MFT | Master File Table, a feature of NTFS |
| NTFS | New Technology File System, one of the file systems for the Windows NT operating system |
| RADIUS | Remote Authentication Dial-In User Service, an authentication and accounting system |
| RAS | Remote Access Server |
| RJ-45 | Short for Registered Jack-45, an eight-wire connector commonly used to connect computers onto a local-area networks (LAN), especially Ethernets |
| Serial Port/ PS/2 Port/ Ethernet Port/ USB port | Interfaces to connect external devices to a computer |
| SPI | Stateful Packet Inspection |
| SSL/TLS | Secure Sockets Layer / Transport Layer Security (security protocols) |
| UI | User Interface |
| VPS | Virtual Private Network |
| VVPT | Voter Verified Paper Trail |

# 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 Center's 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 possible. Special thanks to Marcelo Escolar and Ingo Boltz who served as long-term technical advisers throughout the Carter Center's observation process, and whose work, in at times difficult circumstances, formed the basis for the mission's observation.

The Carter Center's specialized technical mission would not have been possible without the hard work and dedication of the Carter Center representative in Venezuela, Hector Vanolli, who worked tirelessly in Caracas to lay the groundwork for the team with the critical support and assistance of Jacqueline Mosquera, Glory Melendez, and Josefina Blanco.

In Atlanta, Dr. Jennifer McCoy, director of the Carter Center's Americas Program, provided guidance, insight, expertise, and advice, which were essential to the project. Kristin García bore long hours and a heavy workload with good humor and grace. Ethan Watson's presence proved indispensable in Caracas.

Lastly, The Carter Center thanks David Carroll and Avery Davis-Roberts of the Center's Democracy Program, who were in charge of the general management of this project.

Many authors contributed to preparing, writing, and editing this report, including Ingo Boltz, Marcelo Escolar, Avery Davis-Roberts, David Carroll, Jennifer McCoy, Hector Vanolli, Raul Sanchez Urribarri, and Maria Fernandez.

# Executive Summary

In response to an invitation from the Venezuelan National Electoral Council (CNE), The Carter Center organized a specialized, technical mission to observe the use of automated voting technology employed in the Dec. 3, 2006, presidential elections in Venezuela. The Carter Center technical mission had two main goals. First, the mission wanted to demonstrate the support of the international community for democratic elections in the Bolivarian Republic of Venezuela; and second, the mission wanted to contribute to a larger project of The Carter Center to develop and update methodologies for observing and evaluating voting systems globally. Consequently, this report provides some comparative perspectives.

Carter Center observers arrived in Caracas on Nov. 22, 2006, after the completion of many of the pre-election audits. However, they were able to observe a limited number of audits and tests in the two weeks prior to election day, as well as election day and postelection audits. Given the late arrival of the mission, the direct observations of the Carter Center observers were supplemented by analysis of the official minutes from those audits that took place prior to the mission's arrival, information received from the CNE, and interviews with representatives of political parties and civil society organizations, as well as with CNE personnel and Smartmatic staff. More detailed observation records, especially of the source code audits and the traffic numbers of the network traffic center observation, are included in Appendix B.

This report is divided into six sections: (1) institutional design and the political context of the Venezuelan electoral process; (2) design and function of the electronic voting system; (3) voting machine security features; (4) result transmission; (5) audit scheme; and (6) conclusions and recommendations.

**Institutional Design and the Political Context of the Venezuelan Electoral Process**

Given that a thorough understanding of the legal and institutional framework for the election is an important aspect of a technical observation, this chapter reviews the design of the Venezuelan *Poder Electoral*, the formation of the CNE, the impact of the new technologies on the CNE structure, and the initiatives taken by the electoral body to increase public confidence in the automated voting system.

According to the constitution and the law, the administration, execution, and supervision of all electoral matters are the responsibility of the *Poder Electoral*, a fifth branch of government. For this reason, the Venezuelan electoral process is within the exclusive jurisdiction of an autonomous state authority. On one hand, this autonomy has facilitated the rapid and widespread adoption of electronic electoral technologies in Venezuela. On the other hand, in a context of high political polarization, the autonomy has contributed to concerns among the opposition about the integrity of the automated voting system, as well as to perceptions of partisanship on the part of CNE directors appointed by a government-dominated legislature.

Venezuela first piloted electronic voting technologies in its 1993 elections and on a wide-scale basis in its 1998 elections. In 2004, direct electronic recording machines (DREs using touch-screen technology) were introduced with the intention to eventually achieve a totally automated voting system, including voter identification, vote casting, transmission and tallying, and candidate registration.

Before the 2006 elections, the CNE, in extensive consultation with opposition representatives, adopted a number of proposals to strengthen public confidence in the process, including (a) conducting a series of

pre- and postelection audits, (b) conducting a hot audit of 54 percent of voting tables on election day, (c) disconnecting the voting machines during election day, and (d) printing out a record of votes cast in each machine before transmitting results.

The automated system has achieved a good level of technical performance. To ensure sustained public confidence in the system and to avoid the need for repeated ad hoc negotiations, we suggest incorporating many of the measures into standard regulations.

**Design and Function of the Electronic Voting System**

This section examines the diverse details of the Smartmatic voting machines in use during the 2006 presidential election, focusing particularly on the machines' function during election day and the usability and design of the machines.

The Carter Center found the machines to be functioning correctly, which enabled voters to cast their votes with little impediment. Nevertheless, some issues related to the design of the machines were observed, such as confusion among voters regarding the paradigm shift between choosing a candidate using the touch pad and choosing to cast a blank ballot on the touch screen. Another issue observed was the apparent lack of procedures in place for vote correction should the 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 that limited the amount of time available for every voter to vote.

**Voting Machine Security Features**

In this section, both the technical and physical security measures implemented on the Venezuelan electronic system are assessed. The Center found that the CNE took reasonable steps to secure the machines, including encryption of the voting information stored in the machine memories, the use of randomization mechanisms to prevent vote sequence reconstruction, and paper receipt security measures.

In addition, the CNE has 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 República* 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.

**Results Transmission**

In this section, the means of transmitting the votes from the polling stations to the central tabulation center (the central tally system itself) and the security measures in place to protect the vote transmission and tabulation system are analyzed.

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 on the transmission of votes from the voting machine to the tally center. However, the mission found it more difficult 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.

**Audit Schemes**

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. Given its depth and extensiveness, it can be said that the audit scheme

implemented for the December 2006 elections has the potential to become a robust analytical tool for ensuring the integrity of the electoral process.

To achieve this objective, The Carter Center suggests that diverse measures be taken during the pre-electoral stage as well as during the electoral and postelectoral stages. These might include a mandatory comparison of the paper receipt count to the electronic voting results during the election day hot audit, the prior determination of a margin of error and confidence level for audit samples in advance of the audit, and the allowance of the results of a paper ballot recount to form the basis of a legal challenge to the electronic election results. In the pre-electoral stage, the implementation of a series of measures aimed at enhancing procedures could substantially contribute to the achievement of the objectives of the pre-dispatch audit (or *auditoría pre-despacho*).

**Conclusions and Recommendations**

Due to the size and the duration of its specialized technical observation mission, The Carter Center was not able to produce a comprehensive evaluation of the electoral process or of the integrity of the electronic voting system in use in Venezuela. However, taking into account those aspects of the electronic voting system that the mission was able to analyze and observe, the conclusion section offers a detailed series of recommendations aimed at strengthening those aspects of the electoral process linked to the automated voting system to improve the performance of that system in the future.

# About the Carter Center Specialized, Technical Observation Program

In response to an invitation from the Venezuelan National Electoral Council (CNE), The Carter Center organized a specialized, technical mission for the Dec. 3, 2006, presidential elections. In accordance with the Declaration of Principles for International Election Observation, signed by more than 20 international organizations at the United Nations in October 2005, election observation missions may be either comprehensive missions intended to evaluate an electoral process as a whole, or they may be specialized, limited missions to focus on particular aspects of the process.

In this case, the Carter Center technical mission observed the use of automated voting technologies in Venezuela. The mission had two principal goals. First, it sought to demonstrate the support of the international community for democratic elections in the Bolivarian Republic of Venezuela. Second, the mission wanted to contribute to a larger project of The Carter Center to develop and update methodologies for observing and evaluating voting systems globally.

Ideally, The Carter Center would have been in Venezuela well in advance of election day to observe all audits and pre-election tests sponsored by the CNE. However, issues such as the relatively late invitation from the CNE (dated Oct. 9, 2006) and fund-raising demands prevented The Carter Center from organizing a mission within the most desirable time frame.

Carter Center observers therefore arrived after the completion of many of the pre-election audits and only were able to observe a limited number of audits and tests in the two weeks prior to election day. Given these circumstances, the direct observations of Carter Center observers during the pre-electoral stage were supplemented by information received from the CNE, the technology vendor (Smartmatic), political parties, and civil society organizations.

Due to the focused scope of the specialized, technical mission, on election day Carter Center observers were deployed to stations specifically chosen so that observers could assess the influence of social, cultural, and environmental factors on the usability and performance of the voting machines and on the implementation of election administration procedures. Specifically, the observation focused on the impact of human factors (voter wealth and education level, the degree of political polarization, and the degree of political participation) and different results transmission methods (by fixed telephone line, by mobile connection, or physical transmission to the contingency transmission center) on events in polling stations (see appendices).

Due to time and human resource constraints, the Carter Center mission has not produced a comprehensive evaluation of either the electoral process as a whole or of the integrity of the electronic voting system used in Venezuela. However, the Center offers this report, which summarizes the findings of the mission with regard to the functioning of the system during the Dec. 3, 2006, presidential elections based on a comparative analysis of systems used in other jurisdictions. The report concludes with several recommendations.

# 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 "Electoral Authority" (*Poder Electoral*).

Consequently, the electoral process in Venezuela falls within the exclusive jurisdiction of an autonomous state authority.[4] 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 "capacity paradox" (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 "capable" 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 state authority;
- the capacity to recruit staff through the Electoral Service; and
- control of all the stages of the electoral process: civil registration; electoral registration; regulation of political organizations, campaigns and funding; election candidacies and registration of political affiliations; election day procedures such as voter identification, and the casting, tally, transmission, counting, and electoral communication of votes; official announcement of elected candidates; and administrative control and supervision of the electoral process, including the capacity to declare the elections totally or partially void.

In addition, the Electoral Authority regulates all electoral issues not provided for in the constitution, pertinent laws, or through CNE decree or regulation.

## National Electoral Council

The Electoral Authority's main organ is the National Electoral Council, or *Consejo Nacional Electoral* (CNE), which acts as the governing body for all electoral matters in Venezuela. The CNE is composed of five rectors who hold office for seven years and a secretary who is elected by the rectors. The body is chaired by a rector appointed at a plenary meeting from among its members. Each rector has two alternate members.

Its subordinate bodies are as follows:

- The National Electoral Board, or *Junta Nacional Electoral* (JNE), a collegiate body with two regular members and an alternate member of the CNE. The JNE is responsible, among other functions, for planning and executing elections and referenda, and may make proposals to the CNE with regard to election administration.
- The Civil and Electoral Registration Committee, or *Comisión de Registro Civil y Electoral* (CRCE), a collegiate administrative body of a decentralized nature. Members include the heads of those agencies responsible for the civil and electoral registration process, as well as regular and alternate members of the CNE. The CRCE is entrusted with the administrative management of the civil and voters registries.
- The Political Participation and Funding Committee, or *La Comisión de Participación Política y Financiamiento*, a collegiate administrative body of a decentralized nature. Members include the heads of the agencies responsible for the promotion of political participation and the supervision and funding of political organizations, as well as regular and alternate members of the CNE.

In addition, there are other subordinate regional and municipal bodies such as the regional electoral offices and regional, municipal, metropolitan, and parochial boards.

**Composition and Selection of Rectors**

The constitution provides for the participation of three institutions in the selection of rectors to the CNE:

- The Citizens' Power is entitled to nominate one rector.[5]
- The law and political sciences schools of national universities are entitled to nominate one rector.

5 The Citizens' Power (the fourth state power) is formed by the Republican Morals Council: the ombudsman, the attorney general, and the general comptroller office.

- An ad hoc entity, the Electoral Candidacies Committee, or *Comité 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 "small committee" of the constituent assembly (*el 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]

Even though the current CNE is the first designated following the constitution's appointment procedure, the sudden opposition boycott of the December 2005 legislative elections—only three days before the elections—meant that the National Assembly appointing the new CNE in 2006 was entirely controlled by government allies. Consequently, the resulting CNE board was perceived by some sectors of Venezuelan society to be dominated by government sympathizers, which, from the viewpoint of such sectors, has a negative impact on public confidence in the electoral process.

## Introduction of New Technologies

Venezuela began using automated voting on a pilot basis in 1993 and on a widespread basis in the 1998 elections. In the years following, Venezuela increased its interest in the use of this technology.[9] The absence of significant bureaucratic and political obstacles to the administrative management of the CNE (such as budgetary restrictions or controls on behalf of the National Assembly or specialized state agencies) has facilitated rapid incorporation of new information and communication technologies (ICTs) on a wide-scale basis, including not only the act of voting, but also transmission of the vote, identification of the voter, and registry of candidates. As a result, the process has become increasingly sophisticated and has, in the end, achieved good technical performance.[10] However this process of rapid incorporation can also cause uncertainty among key stakeholders as the information gap concerning its use becomes wider.[11]

6 The committee is formed of 11 deputies elected by Congress who then nominate 10 candidates from different sectors of civil society. Together, these 21 individuals nominate three rectors, who are elected by a two-thirds majority of the National Assembly.

7 For example, in the "Herman Escarra and others" case, decided on 08/04/2003

8 Decision of 08/25/2003

9 Article 154 of the Organic Law of Suffrage and Political Participation establishes that the voting, counting, tally, and adjudication processes will be "completely automatic," leaving a manual system only for cases in which the automatic system could not be implemented "for reasons of transportation, safety, services infrastructure." Such cases have to be expressly determined in advance by the CNE.

10 This is in contrast to Brazil and Belgium, where the process was more gradual. In other cases, such as in Mexico, Australia, and Argentina, electoral organs have been opposed to rapid automation (Instituto Federal Electoral of Mexico, Camara Nacional Electoral of Argentina, and the Federal Electoral Office of Australia). Therefore, the introduction of technologies has taken the form of trial-and-error tests at the regional level to develop and study the use of alternative technologies in real voting situations, in some cases with self-developed technology (Canberra 2002 and 2004, Buenos Aires 2005), in others, with proprietary technology (Ciudad de Mexico 2004, Ushuaia 2003).

11 In comparison, in the case of Brazil, the technical sophistication is lower than in Venezuela but consensus has been reached with regard to the technical solution implemented, and there is agreement among political actors and civil society that automation represents an improvement of the electoral process.

This transition has not always been smooth, as evidenced by the changes in automated vote-casting devices used between 1998 and 2006. The initial choice of an optical scan system for the 1998, 1999, and 2000 elections was followed in the 2004 referendum by a system with direct electronic verification and registration (using touch-screen machines). For the 2005 legislative elections, an electronic ballot and direct vote registration system through automated means was used. In addition, biometric registration and identification procedures were officially implemented for the 2004 referendum and regional elections in the "thumbprint machines,"[12] but have subsequently been limited to use as a complement of the voter identification process.

*International experience suggests that the incorporation of ICTs into electoral processes also should entail broad consultation of all political actors.*

The adopted technological model is intended to achieve total automation of traditionally manual voter identification, vote casting, transmission, and tallying procedures of the Venezuelan electoral system, following the applicable constitutional and legal framework.

The normative purpose of these legal and constitutional provisions is, among others, to improve the performance and quality of traditional procedures, making them more secure and reliable, speeding up the results, and ameliorating voting conditions. However, it is important to note that international experience suggests that the incorporation of ICTs into electoral processes also should entail broad consultation of all political actors. Otherwise, the automation process might lead to unintended results, such as increasing uncertainties about the technology among political actors who do not participate in the technological decision-making process.

## Impact of Technologies on the Administrative Bureaucratic Structure

The continued incorporation of new technologies into the different stages of the electoral process has directly affected the bureaucratic-administrative structure of the CNE in the following three ways.

*By reinforcing the centralization of the management of the electoral process.* Automation requires that all logistics, organization, and information-related decisions be concentrated in a decision-making center that is able to guarantee the unified, coordinated, and replicated operation of the devices and systems being used. It must ensure their security as well. This has tended to have a direct impact on the organizational structure of the CNE in that technological areas benefit from an increased allocation of resources. In addition, the role of the chairman and his or her direct subordinates (the heads of the different executive areas of the organization) was strengthened.

*By increasing the average technical level of public agents in charge of the different stages of the system and widening the information and knowledge gap among different administrative areas.* The adopted technological solutions are becoming more sophisticated and are used in more regions of the country. Meanwhile, the staff necessary for maintaining these solutions during nonelectoral periods and for supervising their operation during the electoral process is rapidly growing, not only in numbers, but also in the levels of technical training necessary to fill these roles.

Technical staff members are now also performing many different functions in the electoral process. The concentration of responsibility within this group has reduced the authority of traditional polling staff as decisions are made higher in the electoral hierarchy. This has particularly impacted those responsible for traditional logistical and organizational activities during the elections, as well as those intermediate-level staff in polling stations and in municipal and regional centers of the Electoral Authority.

12 CNE, resolutions no. 04811-1104 of Aug. 11, 2004, and no. 041022-1621, of Oct. 22, 2004

*By reducing the direct management of the electoral processes through outsourcing*. While the introduction of automated solutions tends to enlarge the areas of electoral authorities in charge of technology, the need to outsource the administration of certain aspects of the electoral process to specialized companies tends to make those authorities somewhat dependent upon the services provided by such companies. In the case of the CNE, it initially depended on Smartmatic, the vendor of the electoral machines. However, this dependency has decreased steadily in recent years, as a result of the CNE's greater involvement in all areas of the electoral process, either through direct administration of such areas or by performing a supervisory role.

*The current CNE has taken important measures to continue, strengthen, and expand dialogue and communication between the electoral authorities and opposition representatives.*

For instance, the Electoral Authority is now fully in charge of training voters, table officers, and operators at different levels (initially in the hands of Smartmatic). On the other hand, Smartmatic is still in charge of setting up the platform of the automatic vote, the organization of the technological infrastructure, collecting and distributing the equipment, providing technical support at a national scale, and the management of projects and financial services of projects related to the election. With respect to the technological platform, Smartmatic provided the infrastructure until 2004. Thereafter, it provided additional equipment to satisfy the requirements resulting from an increase in the electoral registry. The CNE now owns its technological infrastructure and takes care of providing the equipment required for each election.[13]

## Technological Management, Trust, and Transparency

To promote public confidence in the democratic process, the new automated processes require steps to mitigate the distrust of those political and institutional actors not involved in the decision-making process, management, or administration of the elections.

Manual electoral processes generally rely on standard administrative protocol procedures that must be complied with as the electoral schedule is executed in order to build public trust. These procedures include the chain of custody of electoral supplies (*cotillón electoral*) and documentary records used for voter identification. In addition, the chain of custody and the decentralized control of the electoral process take place at voting tables during the casting and manual counting of votes where the public can see what is happening.

However, with respect to automated systems, the need to have complex and commonly outsourced systems of logistic administration make it difficult, in practical terms, to comply with constitutional requirements that chain-of-custody procedures be decentralized and participatory in order to be regarded as transparent. These traditional confidence-building efforts must be supplemented by confidence-building measures specific to the new technologies.

Therefore, to increase the transparency of the electoral process, appropriate technical audit mechanisms for the automated components must be developed. These audits must comprehensively cover all aspects of the adopted system and must be based on complete and detailed architectural knowledge to be meaningful. This should be the criteria employed

13 The CNE has chosen so far to purchase what, in its view, makes economic and strategic sense, subcontracting Smartmatic and other vendors for those issues that require high technological specialization, which are not basic needs of the CNE. According to a high officer of the company in an interview with the Carter Center team, it often makes more sense for the CNE to request Smartmatic's services when needed (once a year), than to organize something like an "internal Smartmatic," which would imply more costs and demand steep management requirements, but which would be idle during the nonelectoral periods.

to analyze the audits plan carried out by the CNE during the 2006 elections (see Audit Schemes section).

**Process of Dialogue with the Opposition**

The current CNE has taken important measures to continue, strengthen, and expand dialogue and communication between the electoral authorities and opposition representatives that began during the electoral processes following the 2004 recall referendum. On April 29, 2006, the CNE board made a public call to all of the country's political sectors, with a view to "making sure that the guarantees and conditions existed to allow the participation of the citizenry on Dec. 3,"[14] and then officially opened the consultation process on May 10 (the deadline for petitions to the CNE on behalf of political parties was set at July 31, 2006).

According to information provided by CNE officers, 17 precandidates and 38 political organizations took part in this process of dialogue. During this time, some 55 proposals and requests were filed with the CNE accepting and approving 76 percent of them, according to official information.

Among the most important decisions taken with a view to strengthening the level of public confidence in the electoral process and improving citizen participation was the decision to conduct a hot audit on between 53 and 55 percent of the *mesas de votacion*, or voting tables, on election day (see Audit Schemes section). Another measure with a similar impact on public confidence was the decision to continue the enhanced transmission security processes agreed on in past elections, such as keeping the voting machines disconnected during voting hours (to prevent unauthorized transmissions) and printing out a record of the votes cast in each polling station before the machine started transmitting the results to the tallying center.

In the same round of consultations it was agreed that a comprehensive audit of the complete voting platform, with the participation of political parties and domestic and international observers, would take place together with a revision of the audit protocols. These decisions made possible the ambitious auditing plan of the automated voting system before, during and after the December 2006 elections (see Audit Schemes section).

Another critical measure adopted by the CNE to ensure the transparency of the electoral process was to give representatives of opposition political parties a CD-ROM with the list of all the *actas* counted until that time, an hour before the first official announcement of the results. This measure allowed political parties participating in the elections to check the election results table by table.

All of these measures had an important impact on public confidence. However, they were adopted on an ad hoc basis for each of the electoral processes. The Carter Center mission believes that public trust could be greatly enhanced if the majority of the measures agreed upon were incorporated into the CNE's standard regulations, thus avoiding the need for new agreements for each election.

**Summary of Recommendations**

- Include the procedures agreed upon by the CNE and political groups in the past electoral processes into the Electoral Authority's regular rules and standard operating procedures.

14 Official information provided by the CNE

# 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.

Smartmatic SAES 3000

Smartmatic SAES 3300

***Figure 1: Smartmatic SAES 3000 and SAES 3300 voting machines***

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.

**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 machine's 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 machine's PS/2 ports). The ballot options are printed on a paper ballot that is placed over the touch pad's 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.

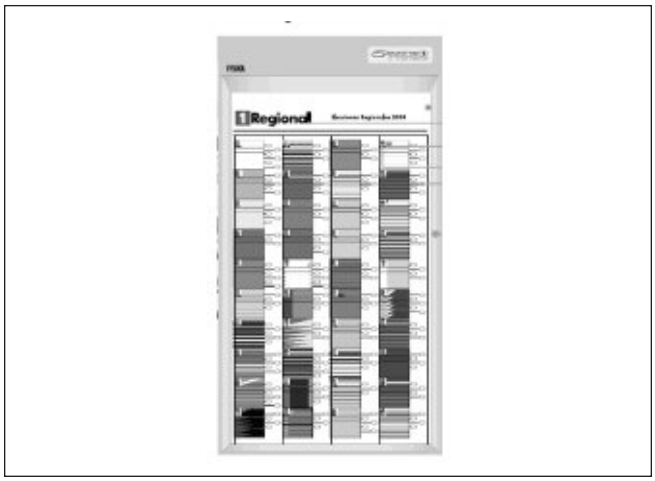


*Figure 3: Touch pad containing ballot options*

**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.

***Ballot option presentation***

After the machine has been unlocked, the voter reviews the available ballot options on the paper ballot sheet that is placed on the machine's touch pad. Every option contains a small photo of the candidate, the candidate's name, and the party name.

***Ballot option selection***

The voter presses a small oval next to the party/candidate of choice, which triggers the corresponding touch-pad button underneath. Once pressed, an enlarged image of the voter's choice (photo of candidate, candidate name, and party name) appears on the touch screen of the voting machine. If the selected image does not reflect the candidate the voter wanted, he or she has the option of pressing another candidate's button on the touch pad, which will change the image displayed on the touch screen until the desired candidate is selected.

Because the touch pad lacks a specific button to cast a null vote, the voter who wishes to do so has the following options:

- He or she does not press any of the candidate's buttons on the touch pad. In that case, the touch-screen area where the voter's choice would appear remains blank.
- If the voter has already selected a candidate but then changes his or her mind and decides to cast a blank ballot, he or she needs to tap the image of the currently selected candidate on the touch screen. This will make the image disappear and replace it with a blank space.

***Vote confirmation***

With the image of the selected choice visible on the upper half of the touch screen (or blank in the case of a null vote), the voter presses the "vote" button on the lower half of the touch screen. In those cases where no candidate is selected, the machine asks the voter to confirm his or her choice. ("Are you sure you want to cast a null vote? Yes/No.") Conversely, if a candidate was selected, pressing "vote" directly confirms the vote. The choice cannot be undone.

***Vote storage***

In case of contingencies, each vote is stored electronically in two different places: in the internal disk on memory of the machine and in the removable memory stick connected to the USB port.

***Paper trail***

After the voter has confirmed his or her vote on the screen and the vote has been stored electronically, the machine prints a paper slip displaying the chosen candidate and party. Unlike the paper on the ballot touch pad and the image on the touch screen, the paper slip does not contain an image of the candidate. The president of the table asks the voter to verify that the paper slip correctly displays his or her vote, fold the paper, and deposit it in a cardboard ballot box.

There are no contingency procedures stipulated for cases in which the voter claims that the paper does *not* accurately represent his or her vote. The electronic vote cannot be cancelled after it has been confirmed on screen and the voter is obliged by polling station procedures to deposit the slip into the ballot box in any case.

***Inking***

After depositing the paper slip, the voter's little finger is marked with indelible ink by a table member as an additional safeguard against multiple voting. After this is done, the voter leaves the polling station.

**During Closing of the Polling Station**

At the end of voting, the table authorities should close the table and finalize the voting process on the machines. The following steps are performed:

- The voting machine operator again enters the unique password to access the operator menu.
- The voting machine operator presses the "close voting" button and confirms this choice with the unique password. Once closed, voting cannot be reopened using that machine.
- The voting machine operator prints out six precinct count reports. Four are handed to the political parties' witnesses.

- 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 voting slip during the election day audit.[20]
- The machines and documents are packed into their respective transport packaging and handed over to the military to be returned to central storage.

**Other Procedures**

There are various other procedures before and during voting day, such as nontechnical procedures during the opening, use, and closing of the voting table, and procedures during election day audits (also known as "hot audits"). They will not be covered in this section as it is primarily intended to illustrate the functioning of the machine itself not the complete electoral process.

**Automatic Fingerprint Identification System**

Before casting a vote in a number of polling stations, the elector should proceed to identify himself or herself through the Automatic Fingerprint Identification System (AFIS).[21] The description of this system is not included in this report because it is not part of the automated voting system. Moreover, its use is not a legal requirement for casting a vote.

## Principal Findings on Voting Machine Usability and Design

During the observation of the automated voting system, the Carter Center mission found that the machines were generally functioning correctly and that voters did manage to cast their votes without impediment. However, the mission believes some aspects of the machine design could benefit from further consideration.

Using a touch pad and touch screen at the same time might have confused some voters. As mentioned previously, when casting a vote, the voting machine established the touch pad as the place where the voter selects his or her choice, and the touch screen as the place where that choice is visually displayed and actively confirmed. For null votes, however, the machine changes the paradigm; the touch pad plays no role and the touch screen acts as both the place where the voter selects and confirms his or her choice. On election day, the mission observers noted several cases where this was a cause of confusion among some voters who alleged that they were not able to cast a null vote or that they had accidentally cast a null vote, possibly due to this paradigm shift. Although the proportion of null votes was negligible,[22] The Carter Center suggests that the CNE consider abolishing the change of paradigm from the user's interfaces to cast a null vote.

As mentioned above, to finish casting his or her vote, the voter was required to manually retrieve the paper ballot slip, verify that it correctly reflected his

19 The printout is not sequential to avoid the reconstruction of the voting sequence.

20 The printing out of these copies is not part of the standard procedure as defined in the operating manual for the table authorities, but it is part of the operators manual.

21 The AFIS was used only in a handful of states and only in those polling centers that exceeded 700 voters. The main goal was to add more fingerprints to the voters' central registry for future use and to speed up the orientation provided to voters in the polling centers, informing them in what page of the voting logbook (required by law) they will find their names.

22 According to CNE figures, the percentage of null votes was 1.35 percent of the total votes (about 160,245 votes).

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—both the electronic vote and the paper vote—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 "cancelled" 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 didn't 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 "null vote" 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 "two times, three minutes" 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 LOV 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.

# Voting Machine Security Features

There are several important security features implemented in the Smartmatic machine design:

- encryption of the voting information stored in DOM/memory stick;
- randomization mechanisms intended to prevent reconstruction of the voting sequence;
- "marrying" of the vote-containing memory stick to the machine to which it is connected during initialization, preventing the original memory stick from being swapped with another;
- disabling any ports not needed for standard operation during voting day and removal of their drivers from the operating system;
- paper receipt slip security;
- voting machine chain-of-custody procedures.

In addition, there were several procedural safeguards implemented in the December 2006 elections to promote the physical security of the machines, such as the use of tamper-evident seals on machine boxes and, in some cases, machine ports and chain-of custody procedures.

## Encryption of Voting Information Stored in DOM/Memory Stick

Each vote cast in a voting machine is stored as a separate, encrypted file in the New Technology File System (NTFS) of both the DOM and the memory stick. The encryption used is a symmetrical algorithm (AES 256-bit), whose password is unique to each machine and is randomly generated during software installation. According to CNE/Smartmatic documentation, "The seed for the password generation is a shared master password, half of which is known to the CNE and the other half is known to the political parties' representatives." [25]

The Carter Center mission applauds the choice of standard industry encryption algorithms such as AES-256 over proprietary solutions. This decision increases transparency and overall system security. However, the random generator used to create machine passwords is also important.[26]

For each voting machine password to be truly random, the seed value fed into the password generator algorithm should be different each time and random for each password created. Commonly used seed values include the computer clock time or a mixture of environmental variables such as CPU and hard disk temperature at the time of password generation. Carter Center observers could not determine if such random seed values were actually used. If a constant non-random seed value were to have been used instead, this would reduce the security of the solution considerably.

## Randomization Mechanism to Avoid Reconstruction of the Voting Sequence

In order to avoid any reconstruction of the voting sequence (through original file attributes or physical location on the storage medium), the system performs the following steps:[27]

- Each vote is saved using a randomly generated file name. The original date and time stamp is replaced with a standard value identical for all the vote files (date of election, time of machine opening).

25 Smartmatic, "Smartmatic Automated Election Systems —SAES_v3.2 101006.pdf" (2006) page 9

26 Since it was not possible to collect information about this practice in Venezuela, this report only offers a theoretical analysis.

27 CNE (2006a)

- Each time a vote is cast a random number of empty dummy files are created and saved first. The actual file containing the vote is then saved after these empty files. After that, the dummy files are deleted.
- The varying space left by the deleted dummy files is used by the next dummy files and the next vote file.
- Because the number of dummy files is random, there is no way to predict or reconstruct the physical position of the next vote file on the hard drive. For example, if fewer dummy files are generated, both these dummy files and the second vote file may be saved somewhere before the first vote file. If, conversely, more dummy files are created, the second vote file may be saved somewhere after the first vote file, and so forth.

During the run-up to the December 2005 legislative elections in Venezuela, while carrying out one of the voting machine audits, a potential method to reconstruct the voting sequence using the records stored in the NTFS Master File Table (MFT) was discovered. In response, an additional measure was added to the randomization procedure. The complete content of each folder of the file system is renamed twice, at various times during the voting day. This removes the access traces left in the MFT. At the end of the voting day, all the system's MFT records show access time stamps close to the closing time of the table, making sequence restoration impossible. The Carter Center mission finds this method to prevent voting-sequence reconstruction comprehensive and secure. In fact, the mission does not know of another electronic voting system—including those used in Brazil, Belgium, Australia [Canberra], and India—where such emphasis has been placed on possible reconstruction of voter sequence from analysis of the HDD file system.[28]

## 'Marrying' of the Memory Stick to the Machine

According to the head of the Informatics Department of the CNE, the inserted blank memory stick is "married" to a specific machine during installation of that machine, making it impossible to replace memory sticks. According to Smartmatic, when a memory stick is inserted into a blank machine for the first time, it transmits a unique password to the machine.[29] From then on, votes both in the machine's DOM and in the memory stick are encrypted using an AES-256bit encryption algorithm and that unique password.

According to documented CNE contingency procedures, in cases where a faulty memory stick or a faulty machine needs to be replaced, the stick and machine "resync," copying the votes recorded so far to the respective replacement unit so that a complete duplicate dataset is restored. The original password is then used to encrypt the rest of the recorded votes. According to the vendor, this resync process is adequately secured by encrypting the transmission of the original password to the replacement unit using one special password that is identical to all machines and memory sticks.[30]

Further details on the security policies regarding this master password would be useful because these policies will have a significant impact on the security of the system. If compromised, this master password may allow the creation of new blank memory sticks. Upon being inserted into any voting machine, the stick could authenticate itself with that master password to simulate a contingency sync and gain access to each machine's unique password and the votes

28 There are papers that examine other methods of reconstruction of voter identity, such as Brunazo (2004) on the Brazilian case.

29 Smartmatic technical presentation.

30 Only if the password is known by sticks and machines can any contingency device securely sync with any partner component.

stored in its memory. Available documentation does not provide clarity on whether additional security measures have been implemented to prevent this possible kind of attack.

## Physical Security

The main measure preventing physical access to the inside of the machine is a key lock that stops the chassis from being opened. In both models, the components located inside the chassis are the on/off switch and the USB port used to connect the memory stick. On some 3300 models, the observers saw that the memory stick USB port additionally was sealed with a special tamper-evident sticker.

Moreover, in both voting machine models, regardless of the key lock mechanism, a set of ports (serial, PS/2, modem, Ethernet) is easily accessible, either behind a simple plastic cover (3000) or completely uncovered (3300).

According to the vendor, unneeded ports may be disabled in two ways: physically (by not connecting cables from motherboard connectors to the corresponding plugs) or via software (by disabling the ports using the Windows XP registry).

The Carter Center mission did not have information about which ports on the voting machines were disabled and so was not able to conduct a more thorough analysis of the potential for port-based local attack schemes.[31]

During the December 2006 elections, tamper-evident stickers were used in addition to key locks to prevent physical access to the voting machines. The mission observed that such labels, if consistently implemented and comprehensively checked with binding security consequences for violation, can make physical access to a machine or its ports difficult and can act as a deterrent.

On election day, the Carter Center mission observed tamper-evident stickers covering the USB ports of several machines. However, the security procedures regarding these stickers seemed ambiguous. For instance, in the CNE-issued machine operator manual the sticker is not mentioned when describing the process of verifying the presence of the memory stick. [32] Nor are there any prescribed consequences should that sticker be found to have been tampered with, or instructions for resealing the USB port after the presence of the stick has been verified.

Carter Center observers noted inconsistencies in how operators handled the tamper-sticker procedure on election day. Sometimes the port was resealed with a new sticker; in other cases the broken seal was reglued to the port. In yet another case, the port remained unsealed. It was unclear whether operators saw the integrity of that sticker as important, or whether they were aware of procedures to be followed in cases where the seal was broken. The Carter Center observers believe the inconsistent use of tamper-evident seals could leave the machines vulnerable to a security breach via unsecured ports.

With respect to the key of the chassis, it is a simple tubular key without special security features, which means that all machines can be opened with the same key. Due to these characteristics, the Carter Center observers believe that, in addition to the tamper-evident stickers, the use of a nongeneric key, individual to each machine, might improve the overall security. With 33,000 machines in circulation all having the exact same key, gaining access to one such key would not be difficult, particularly because this type of key can be bought freely in the market.[33]

31 There is a significant difference between both mechanisms. Connecting physical wires is a process which invariably needs manual intervention, machine-by-machine. Hence a large scale security attack is unlikely to use this method. In contrast, re-enabling of software-disabled ports is much easier and could, in theory, be achieved by malignant software, introduced centrally by one informed insider. A software-disabled port is hence significantly more dangerous to system security than a physically disabled one.

32 CNE (2006b)

33 This weakness of lock mechanisms has been frequently noted in other international contacts. Consequently Venezuela's system shares this weakness with a large number of other systems worldwide.

## 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 the Electoral Authority using safety ink.[34] They also include a unique, randomly generated 32-character, alphanumeric serial number generated and printed in real time when the vote is cast. Because the seed variables for the random generator algorithm are both machine specific (the code of its geographic location on election day) and random (a mixture of various computer component temperatures at time of code generation), each machine produces its own unique numbers. The Carter Center team assumes that the serial number contains integrity mechanisms such as checksums to prevent forgery. [35]

While this serial number may make it impossible to produce falsified paper slips, its actual practical value is limited because it is not currently possible to machine-read the security code on the ballot paper. Consequently, should the need arise to verify the authenticity of a large number of paper slips using that code, the only method available would be manual visual reading of the complex code and inputting each serial number into a computer system one by one. This might be remedied by the inclusion on the paper receipt of a machine-readable barcode (in addition to a humanly readable serial number). [36]

In sum, although it may be mathematically impossible to forge a correct security code, cases where a large-scale verification of the authenticity of these numbers is required would take a huge amount of human resources and a long time, thereby diminishing its importance as an effective security measure.[37]

## Voting Machine Chain-of-Custody Procedures

Considering the relative ease of access to the machine itself, much responsibility for system security rests on the chain of custody. The chain of custody is intended to prevent unauthorized access to the voting machines during storage and transportation. In Venezuela, this procedure relies mainly on the following:

- a special unit of military active-duty soldiers called *Plan República*, which is formed specifically for elections and is theoretically under direct control of the CNE (rather than the military high command)
- security tamper tape sealing the boxes containing the voting machines during transportation

The central warehouse facility where the machines were configured and their voting software installed was guarded by the *Plan República*, as was their transportation to polling stations across the country.[38]

According to the regulations, before being shipped to their respective polling stations, the machine boxes were to be sealed with CNE security tape. Upon arrival at the polling stations (usually three or four days before election day), the voting machine boxes were not to be opened, but were to remain sealed and stored until the day of the election dry run (in the case of the 2006 elections, until Friday, Dec. 1). On this day, the boxes are to be opened in the presence of the polling station authorities, the technicians in charge of the machines, and members of *Plan Republica* so that completeness of the component inventory and correct functioning of the machine could be verified (running diagnostics). If no problems were found, the boxes were to be resealed with security tape and the new tape signed by the table authority members.

34 Details of the composition of the "safety ink" could not be determined.

35 Available documentation did not provide specific details.

36 Smartmatic states that their system is capable of producing such a barcode, but the CNE did not request that feature.

37 Having said that, there is little material available indicating that in other electronic voting systems there is much emphasis on mechanisms to prevent forgery of paper slips (if they use them at all). Hence this additional measure, while of little use, does not devalue the security of the Venezuelan paper slips in international benchmarking.

38 The logistics and means of transport (trucks, etc.) are provided by AEROCAV, a private company contracted by Smartmatic.

Finally, on election day, (again in the presence of the table authorities and party witnesses), the boxes were to be opened and the machines installed and used. After the end of voting, the machines were to be returned to the boxes, the boxes resealed with the security tape and the new tape again signed by the table authority members. The sealed boxes, with machines inside, were to be shipped back to the central logistics warehouse for possible audit and storage.

If the military in charge of machine custody comply with their duties following the applicable electoral regulations, and the procedures for tamper-sealing the machine boxes are performed in a comprehensive manner, manipulation of the machines in transit should be fairly difficult to achieve.

*If procedures for tamper-sealing the machine boxes are performed in a comprehensive manner, manipulation of the machines in transit should be fairly difficult to achieve.*

However, this process may benefit from greater clarity about the procedures and increased supervision. For example, neither the manual for the polling station authorities[39] nor the manual for the *Plan Republica*[40] contained instructions on how to verify the integrity of the tamper-evident tape upon receipt of the machines on the day of the election dry run (when the boxes are first opened after being shipped from the central warehouse) or on machine setup on election day.[41] Only the short manual for the machine operators[42] contained instructions on the verification of the tape on machine reception in both occasions. However, it did not define obligatory responses other than "calling the technical support center" in cases of violation. The generally accepted practice is that responsibility for the chain-of-custody and security procedures should be shared among all stakeholders.[43]

At the end of the voting day, The Carter Center observers noted several cases of confusion among table authorities about prescribed procedures for sealing the boxes containing electoral documents.

For example, the following was observed:

- Table authority members, when sealing the boxes, signed the cardboard of the boxes instead of the borders of the tamper tape. Because the tamper tape itself was available in polling stations and not particularly securely guarded, the best safeguard against someone simply removing the tape, manipulating the box contents, and resealing it with new tape was the table authorities' signatures across the borders of the original tape (falsifying signatures is more difficult than replacing tape). In cases where only the boxes were signed, but not the tape, this security procedure was rendered ineffective.
- Table authorities sticking tamper seals on solid sides of boxes instead of across the places where these boxes could be opened. Again, opening the boxes in these cases would not require breaking the seal. Therefore a "sealed" box could be manipulated unnoticed.

39 CNE (2006c)

40 CNE (2006d)

41 Both manuals do contain instructions on sealing the boxes after the dry run or the closure of elections

42 CNE (2006e)

43 Please see the section summarizing The Carter Center's observation of the election day dry run for more information.

While these incidents do not prove that any manipulation occurred, they do show that it is theoretically possible. To correct this problem, physical machine lockdown and chain-of-custody procedures should be improved in future elections. These incidents underscore the importance of consistent application of the chain-of-custody security measures.

As a general concern, the heavy reliance on the military to provide secure custody of the machines raises questions. The military, because it is commanded by the executive, is not necessarily impartial. Even though the *Plan Republica* military staff is theoretically under the direct control of the CNE during elections, The Carter Center observed several cases where superior officers overrode CNE instructions, relying instead on the traditional chain of command.[44] Even if the CNE had full control, some sectors believe the CNE is dominated by sectors close to the government. Greater participation of civil society, and especially the opposition, in machine custody is desirable.

**Summary of Recommendations**

- Make the paper ballot serial number machine readable. By doing so, the serial number becomes a functional security feature that can be verified during a paper recount with a reasonable amount of effort.
- Clarify physical security procedures and require their consistent application. These measures would allow table authorities, poll workers, machine operators, and Plan Republica officers to more easily ensure the physical security of the machines and would make the use of tamper-evident seals a more meaningful security procedure.
- Improve transportation and storage chain-of-custody procedures This might include broadening responsibility for security of the technologies during installation and storage to include political parties and civil society groups.

44 In this case, a superior prohibited a junior officer from following CNE procedure and accompanying the table president and witnesses to a Contingency Transmission Center (CTC) after regular transmission from the polling place had failed. Even direct calls to higher CNE authorities, who confirmed the correctness of the procedure and instructed the junior officer to do as he was told by the table authorities, were disregarded.

# Results Transmission

According to the procedures established by the CNE, after the end of voting and the closing of the table, the votes stored locally (both in the machine's DOM and the memory stick) during the voting day are transmitted electronically to the central tally server.[45]

Several channels were used to transmit the results:

*Fixed telephone line*. This was the standard transmission method used in the majority of the polling places. Following the norms approved by the electoral authorities, after voting had finished, a phone line was connected to the voting machine's RJ-45 modem port. The machine should have then dialed into a remote access server (RAS) to establish a connection once the line was validated (against the "white list"),[46] and the machine was successfully authenticated against an authentication, authorization and accounting (AAA) server. After the connection was established, the machine should have begun transmission through the central tally server at the CNE (the reception server). If reception was not possible after two attempts, the transmission was terminated (and an error message displayed at that time). Voting machine operators could repeat that procedure as many times as they saw fit. If successful transmission was not achieved, they then switched to mobile phone transmission, and failing that, manual transportation of the memory stick to a Contingency Transmission Center (CTC).

*Mobile telephone line*. Mobile telephone was the standard *contingency* transmission method used in the majority of the polling places, where transmission using the fixed line ultimately failed. In some polling places, a mobile transmission was the only planned transmission method because fixed lines were not available. For this method, a mobile telephone provided by the CNE to the operators of the voting machine was used. The approved procedure in this circumstance required connecting the mobile phone 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.[47] CTCs in most urban areas used fixed lines.

The network infrastructure was specifically provided for this electoral system by CANTV, the Venezuelan National Telephone Company, whose topography is described in Figure 4.

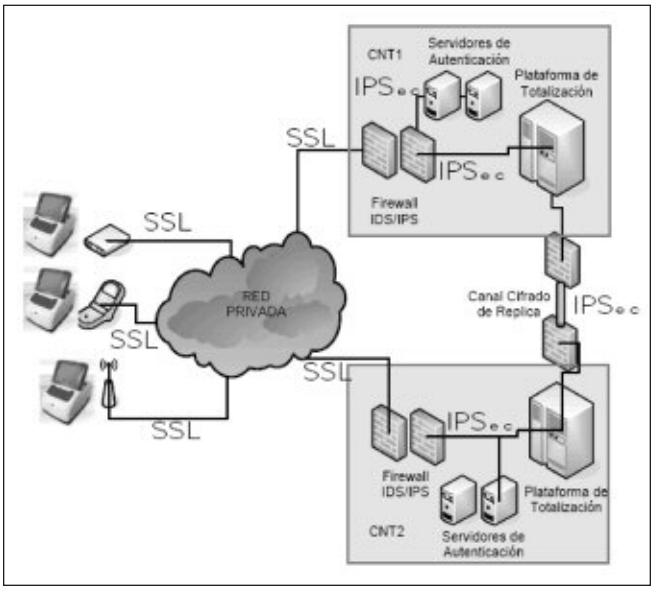


***Figure 4: Transmission Infrastructure Topography (Source: CNE, "SAES_v3.2 101006.pdf," 2006)***

45 Both an aggregated list of voting results (official precinct count result) as well as each individual vote file as stored on the DOM and memory stick, are transmitted to the tally server.

46 See the next section in this chapter for further details on the "white list."

47 There were satellite antennas present in all the polling places that used the AFIS system since the AFIS used satellite transmission as its standard means of communication with the central electronic voter register to store fingerprints. However, the networks were not related or interconnected in any way. The Carter Center mission could not corroborate the location of the satellites. The assistant head of the Electoral Authority's department of computing services communicated verbally to a Carter Center representative that such satellites were not used during the December 2006 elections.

## Transmission Security Measures

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

- *Dedicated infrastructure — (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 "grey candidates," such as cell phones of machine operators who had not been showing up for work.[49] Similarly, for satellite connections, a list of approved "satellites modems" was created. Only accepted modems could communicate into the network.

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

  – The CNE's CNT1 with its contingency CNT2

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

  – 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 CNT 1 & 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 "white list" a day before the election. The audit was specifically designed for this purpose.

during the months before the elections (see Process of Dialogue with the Opposition section), including the following:

- The voting machines may not be connected to any means of communication during voting day, to avoid potential remote influence on the machines.
- At least one of the official precinct count reports generated by the voting machine after voting closes must be printed before connecting the machine for result transmission, to preempt potential remote changes in the machine during result transmission.
- The CNE AAA servers should be deactivated until the National Electoral Board (JNE) authorizes the start of reception. Until then, no IP addresses are assigned to voting machines and no results transmissions accepted.

A detailed analysis of potential attacks on the transmission infrastructure would go beyond the scope of this report. Based on available information, the transmission infrastructure appears to be reasonably well-guarded against outside intrusion.

On the other hand, choices such as using the CNE's own certificate authority, instead of an independent, mutually trusted third party certification provider, may cause unnecessary mistrust among non-CNE stakeholders. In highly polarized political situations, an independent third party certificate authority could inject trust into the whole system.

## Functioning of the Centralized Tally System

According to the regulations in place for the December 2006 elections, all votes should be transmitted after poll closing to the CNE's central tally system using the communication infrastructure described above.

The central tally system consisted of four main modules:

**Election Management System (EMS)**

The EMS was in charge of receiving the election data as input (such as ballot options and polling place information) and from that generating the configuration files for each voting machine. It also generated the unique password to encrypt the vote files and the password needed to activate each voting machine and access the operator menu.


***Figure 5: Tallying system modules (Source: CNE, "SAES_v3.2 101006.pdf," 2006)***

**Party Endorsement Manager (PEM)**

The PEM was used to manage changes of candidate alliances by parties, a standard practice in Venezuela politics. Political parties who initially endorsed a certain candidate for the presidency could change alliance and endorse another candidate in the run-up to the elections. These shifts could occur up until a short time before the elections, even if the paper ballot sheets which were placed on the ballot touch-pad units were already printed and there was little time to reprint them to reflect the change of endorsement.

Consequently, in the 2006 presidential elections, the paper on the ballot touch-pads and the screen confirmation did not reflect any last minute endorsement changes and may have displayed that a vote for party A would result in a vote for presidential candidate B, while in reality party A changed its endorsement to presidential candidate C. An uninformed voter, trusting the machine's display and thinking he or she was voting for candidate B by voting for party A, will in fact have his or her vote counted for candidate C.[50]

50 Voters are then compelled to inform themselves of such changes, e.g. through the media or the CNE's web site, in order to know to ignore the incorrect information displayed on the ballot touch-pads. However, considering that there are a large number of small political parties in Venezuela, many of which remain largely unknown to the public, endorsement changes may well go unnoticed.

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 places' 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, verifies, and passes on individual results transmitted. It does not aggregate voting data.

**Real-Time Electoral Information System (REIS)**

The main goal of the REIS was to provide access to real time election data as the election unfolds on voting day, such as:

- The number of voting machines that had already transmitted
- A display of individual voting files transmitted
- Intermediate results[53]

The REIS was also used to emit bulletins and other official documents. Access to the REIS was protected by a username/password scheme with access rights management. Each user was restricted to see only the information he or she is authorized to see.

**Access by Regional Authorities**

In addition to the voting machines and the direct access from CNE headquarters, the regional electoral authorities in the states also had access to the central tally system, for two functions:

- Tracking progress of voting activities during election day (query results database);[54]
- Submitting transcribed results from the few polling stations using manual voting (2 percent of the total) to the CNT. Specifically, they connected via SSL to the REIS listener module, similar to the way a voting machine would connect.

**Central Tally System Security Measures**

In addition to physical access restrictions to the building and rooms in which the central tally system was located, the security scheme in place for the data-transmission process included the following measures:

51 The machine's user interface on the screen repeats the choice made on the ballot touch-pad, as mentioned earlier.

52 SSL 2048-bit encrypted communication

53 According to Smartmatic (2006a): "SAES facilitates the print-out of tally documents as results are being tabulated… As soon as any tally reports are produced, partial or total, these reports may be published directly on a web site and viewed by the general public." It is unclear to what extent the CNE made use of these system capacities during the elections.

54 Whether this includes the capacity to see aggregated results while votes are still coming in remains unclear.

- All applications that require user intervention were protected by a username/password scheme with access rights management;
- All user and system activity in all modules was logged; and
- Each packet received by the REIS listener was saved, for logging purposes, in a local database of the application server running the REIS listener.

The effectiveness of the access security schemes to all of these central modules is important. For example, a person with access to the PEM module could switch endorsements from one candidate to another—changes that cannot be observed by voters or table authorities in the field (since the machines do not show them). Since many small parties usually do not generate much public attention, "unexpected swings" may not be widely noticed.

Despite the importance of the security measures, the amount of detailed information available on the procedures guarding the central tally system was much smaller than the amount of information available on both voting machine security and transmission security. It would have been useful to have more detailed information on access rights management within the CNE, such as how username/password combinations are assigned to users; who sets the access rights where and how; if and how system activity logs are monitored; and which, if any, response policies exist in case of detection of anomalies. In the absence of detailed information it was difficult to judge the security measures implemented.

## Global Security Discussion

The system used in Venezuela is not modular, but monolithic, both physically/logically and in source code.[55] Therefore, it needs to be secured (and audited, see below) in its entirety. With approximately 200,000 lines of source code[56] plus a full Microsoft Windows XP Embedded operating system, it is a complex system with many potential openings for an attack. A very comprehensive security scheme is necessary to counter that threat.[57]

As described above, encryption and digital signatures have been applied to secure the storage of votes in the machine and their transmission to the CNE. Because the system as a whole is complex and The Carter Center mission was not provided with engineering level specifications and/or the source code, a complete analysis of security weaknesses cannot be attempted here. However, it is important to remark that no system is 100 percent secure, and there are systems that have been shown to be more open to attack than the Smartmatic one as analyzed here.[58]

Therefore, in the specific case of Venezuela, it can be said that a reasonable effort has been made to protect the system against outside attacks on the votes (once stored in the voting machine), and on the transmission of the votes from voting machine to the tally center. In contrast, the degree of security in the

55 There are other systems, such as the magnetic card model used in Belgium and the conceptual model 'FROG' developed by CalTech/MIT (2001), which take a modular approach. In this approach, the first module presents the vote options to the voter, and then registers his/her choice on a medium that the voter him/herself can verify independently. After the voter verifies that his/her vote has been correctly recorded, s/he introduces the medium into the second module. That module reads the medium and transmits (or stores locally) the choice recorded on it. Because there is voter verification of the recorded vote after the first module has completed its work, the software of that module does not need to be extensively secured; only the second module (which reads and transmits the stored vote non-transparently to the voter) needs to be strongly protected against attack. This second module is much easier to audit because it contains simpler source code as most of the system presentation logic and voting user interface (which require a lot of code) are located in the first module. Hence modular systems are much easier to secure than monolithic systems.

56 Estimate of a Smartmatic technician during an interview.

57 In this sense, the switch of technology from optical scanners (used until 1998) to the DRE technology now used has significantly increased the need for security measures, since scanners are an example of a modular system.

58 For example the initial versions of the Diebold AccuVote TS System, whose weaknesses have been exposed by RABA (2004). Please see Tadayoshi, Stubblefield, Rubin, Wallach (2003).

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

For the 2006 presidential elections, the CNE implemented an audit plan which included, among other procedures, pre-election audits, a "hot audit" during election day, and postelection audits. A distinctive feature of these audits was the participation of representatives of political parties taking part in the election, who gave their formal and explicit approval to all procedures put into place. This audit framework is comprehensive and has the potential to become a robust analytical tool for ensuring the integrity of the electoral process.

## Limits Inherent to Audit Processes

By way of an introduction, it is important to note that audit processes are inherently imperfect. In particular, source code audits, arguably the most important part of any audit process, have limited effectiveness in many cases. The software experts in charge of examining the source code must analyze code that has not been created by them, with a large number of code lines. For example, the electronic voting system "AccuVote TS" made by Diebold contains approximately 285,000 lines of source code;[59] the Diebold/Procomp electronic voting system used in Brazil has three million lines of source code.[60] Finding errors in such large quantities of code is like looking for a needle in a gigantic haystack. Moreover, a malicious programmer will always try to hide any manipulations, making them even harder to find.

*This audit framework is comprehensive and has the potential to become a robust analytical tool for ensuring the integrity of the electoral process.*

Given these difficulties, some experts claim that auditors can never be certain that the audited software is 100 percent safe.[61] In any software audit, it is likely that errors will be overlooked. If manipulations in the source code exist, they may well remain undiscovered.

That being said, it is important to stress that designing and implementing a comprehensive audit scheme according to best practice may significantly reduce the chance of manipulation and/or errors.

In order to judge the security of any electronic voting system as comprehensively as possible, three key steps are usually recommended:

- A specified and documented analysis of the electronic voting system's technical design and its security measures to identify and evaluate possible weaknesses and the likelihood of an attack exploiting these weaknesses.
- A thorough inspection of the actual existing system (including both software and hardware), in order to determine whether the technology that is being used during the electoral process conforms to its published specifications; and
- An equally careful inspection of the non-technical procedures carried out before, during, and after the elections, in order to determine whether the actions that were actually performed strictly followed the specified rules and regulations.

59 RABA (2004)

60 Rezende (2004)

61 Computer security veteran Ken Thompson (1984), for example, says: "You can't trust code that you did not totally create yourself… No amount of source-level verification or scrutiny will protect you from using untrusted code… A well-installed microcode bug will be almost impossible to detect." Other experts like Neumann (1993, 1995) and Mercuri (2002) agree with that view.

Ideally, such analysis and possible improvements in response to identified risks will lead to technical security mechanisms (encryption, digital signatures, etc.) and non-technical security procedures (tamper-evident seals, locks, clear chain-of-custody procedures, personnel access policies, etc.) that minimize the risk of the system being manipulated.

Only if an analysis of the systems (technology and processes) results in the conclusion that it is reasonably safe, and the practical observation comes to the conclusion that this exact same system has been used in the elections, can one state with some confidence that the elections were reasonably secure.

## The Audit Scheme Used in Venezuela

The audit scheme implemented in Venezuela in the 2006 presidential elections consisted of a mixture of technical and non-technical audits. Because the Carter Center observer team arrived on November 22, some of the audits had already taken place, so they could not be observed. To remedy this circumstance, The Carter Center mission attempted to partially reconstruct these audits, using both the official minutes of these procedures[62] and informal interviews with audit participants.

The main audit blocks were the following:

- The hardware audit (voting machines)
- The source code audit (both for voting machine and the central tally system)
- The transmission infrastructure audit
- The "machine production audit" and "pre-dispatch audit"
- Election day "hot audit"
- Postelection audit

In addition, CNE technical staff carried out audits of the software and hardware of the Automated Fingerprint Identification System (AFIS). Since the AFIS is not part of this technical analysis and The Carter Center was not present during many of these audits, they are not considered in this report.

Prior to election day, non-technical parts of the voting system were also audited, such as the printed voter registers used for voter identification on election day, and the central voters roll used to generate these registers. Since these elements are only indirectly related to the electronic voting system itself, and because The Carter Center was not present during these audits, they are not covered in this report.

Finally, the vendor also performed several system tests, some of them on a large scale, in order to assure performance of the system. These will not be covered in detail here, as they did not form part of the public audit scheme, and were not observed by The Carter Center.

### Procedure Changes On-the-Go

An important feature of the audit process was its flexibility. Many details of the process were negotiated by the CNE and party representatives during the audits themselves, setting aside what had been previously agreed. From discussions with party representatives and by comparing the official minutes to observation reports obtained from non-CNE sources, The Carter Center mission could infer that a number of questions were posed during these audits, negotiations over audit processes followed, and agreements were reached. Processes were generally adapted according to these oral agreements.

Although this could be considered a good indicator of the willingness of the CNE to respond to the requests and concerns of the political parties, it complicated the audit process because auditors and observers (both domestic and international) could not adequately prepare in advance for the audit sessions.

A frequent complaint by opposition representatives was that the CNE had been unresponsive to their questions and requests and to their petitions for an explanation of the procedures and processes implemented on the Dec. 3 elections. For example, an internet-based forum, a principal tool for pre-audit Q&A and clarifications, was not attended by the

62 CNE (2006f)

CNE and the more than 100 questions posed there remained unanswered. However, the party representatives freely conceded that once the audits were underway, the CNE had complied with their requests for changes and even arranged extra audit sessions not initially planned.

## Pre-election Audits

The audits undertaken during the pre-election day period were the following: Hardware audits; source code audits; transmission infrastructure audit; machine production audit and pre-dispatch audit. The Carter Center mission observed only the pre-dispatch audit and the last day of the machine production audit.

*Controlled source code reviews provided political party and other auditors limited access to the source code. However they were not able to apply their own diagnostic tools.*

**Hardware Audits (Voting Machines)**

According to the official minutes, hardware audits took place on Oct. 11 and Oct. 13. On Oct. 11, technicians from political parties dismantled and inspected the physical components of the 3000 model voting machines and "inspected the operating system." On Oct. 13, the 3300 model was inspected. According to the minutes, a 3300 machine was formatted, and a clean copy of the operating system (Windows XP Embedded) was installed. Then, an image of that installation was generated (using Norton Ghost), and three hashes were generated of that image (MD-5, SHA-I, SHA-256).[63] The hash values were recorded in the minutes. According to the CNE both the 3000 and the 3300 machine run the exact same software, so this set of hash values should serve for both machine types. These hashes would later be used to verify that the same image was being installed on all voting machines without alteration.

**Source Code Audits (Voting Machine Software and Tally Center Software)**

According to the official minutes, source code audits took place between Oct. 16 and Nov. 30, with voting machine software audits being completed by Oct. 31. Tally center software audits were mostly completed by mid-November, with the exception of two extra audit sessions on Nov. 21 and Nov. 30, only four days before the election. Carter Center observers were not present during any of these audits, which (except for the last one) took place before their arrival in Caracas. Carter Center observers were not invited to the last source code audit.

Controlled source code reviews provided political party and other auditors limited access to the source code. However they were not able to apply their own diagnostic tools.[64] According to an informal interview with CNE staff, the opposition auditors insisted initially on using their own tool, but since their tool could not verify hashes in batch, they eventually reverted to using the CNE issued tool. Putting this issue aside, the Carter Center mission believes that transparency and public confidence in the audit process might be improved by increased and more thorough access to the source code by accredited domestic and international organizations and political parties.[65]

**Transmission Infrastructure Audit**

On Oct. 20 and 24, the transmission infrastructure audit took place in the CNE headquarters. According

63 This is an example of the aforementioned ad-hoc changes to the process. Initially, only MD5 was planned; the inclusion of SHA-I and 256 happened in response to demands from the political parties.

64 With the exception of their own tool to generate and verify MD5 hashes.

65 See Rezende (2004) for commentary on a similar process in Brazil.

to the official minutes, it consisted of a presentation of the infrastructure's various modules. From the wording of the minutes, it can be inferred that this presentation was informational in nature, probably using one of the PowerPoint presentations which was used during a similar information session arranged for the international observers of the OAS, EU, and The Carter Center.

Electoral officers orally informed The Carter Center mission that an audit of the telecommunications platform was also performed during this period. This audit included a review of several elements, such as the white list, the configuration files, the routers, the RAS servers used in the CNT1 and the CNT2, and the routes of CANTV, Movilnet, and redescom networks.

**Machine Production Audit**

According to the official minutes, machine production audits took place on each day of voting machine production, between Nov. 1 and Nov. 23. Carter Center observers were only able to observe those procedures performed during the last of these audits.

The main objective of the machine production audits was to select a random sample of 0.5 percent of all the voting machines (or 164 of a total of 32,331 machines) prepared in the assembly facility for later use in the pre-dispatch audit which was conducted on Sunday, Nov. 26. The sample of 164 voting machines that had been selected during these audits were sealed and stored for this purpose.

During this audit, Carter Center observers noted the following:

- The auditors used a randomized sample of machines by "pulling machine numbers from a hat." Although this sampling method contributed to ensuring the transparency of the process, The Carter Center mission recommends that the CNE consider using a more scientific sampling method in the future.
- The size of the 0.5 percent sample of machines selected from the total machine universe seems arbitrary, since the margin of error and confidence level was not clearly stated. Although the procedures leading to the picking of the machines were approved by political party representatives, The Carter Center mission believes that the sampling process would have been more meaningful if the margin of error and confidence levels had been stated in advance of the audit process.
- Auditors did not personally witness the picking of the chosen machines from the production line, but were presented with them in the venue set up for this purpose. According to CNE officers, access to the area where the machines were assembled was restricted for industrial safety reasons. Though this seems reasonable, The Carter Center mission believes that, in the future, the electoral authorities should consider implementing procedures that take into consideration the safety and physical integrity of auditors, to allow them to actively participate in the identification process of the machines in the assembly area.

**Audit of the Touch-pad Production**

On Nov. 3, an audit of the ballot option touchpad production took place. Official minutes indicate that the following procedures occurred:

- Auditors made a random selection of a ballot touch-pad from the production line;
- Auditors verified that the selection produced by pressing the touch-pad buttons coincided correctly with the overlaid image on the paper ballot of the candidate and party.

**Pre-dispatch Audit**

The pre-dispatch audit which took place on Nov. 26 was the most public audit of the series. The audit was designed and organized by the Central University of Venezuela, with whom the CNE contracted for this purpose. Carter Center observers were present at this audit.

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 was conducted in batches. The procedure was to simulate the voting process with the first set of machines (enter the number of determined votes into the machines and transmit them to the tallying servers) and then return the first set of machines to storage, making space for the second set of machines to be audited. The same procedure would then be performed on this group, which would later make space for the third set and so forth, until all machines were tested.

The support technicians proceeded to set up each batch of machines and prepare them for the voting process, following the procedures in place. In addition to the standard procedures for this stage (connecting the ballot unit and the release button, etc.), the technicians connected an external keyboard to each machine through which they accessed a password-protected BIOS configuration menu, where they changed the system time of the voting machines, effectively forwarding it from the actual time (approximately 10:00 a.m.) to 3:00 p.m. The reason given for this by CNE technical staff was that the machines were programmed to prevent voting result transmission before 4:00 p.m. on voting day. Because this audit required earlier transmission (in part to make space for the next batch of machines) it was necessary to change the time.

During the set-up of the machines, The Carter Center mission observers noted that a number of machines showed some minor problems which were fixed by technicians.[69] In addition, they observed that some of the machines were tested with their back cover left open during the audit, which eased access to the voting machine's input/output (I/O) ports (in some cases, there was no seal to secure the back cover). During the whole day of audits, five of the

66 Due to the large number of people and voting machines at the audit hall, it was not possible to observe each and every part of the audit taking place. Observations have the character of spot checks, with observers roaming on the premises and conducting observations and interviews as the various participants became available.

67 The facilities of AEROCAV, in the area referred to as Filas de Mariche.

68 Due to the large number of people and voting machines present at the audit site, it was not feasible to observe every part of the audit in detail. Observations then worked as random controls: observers walked around the place and made observations and conducted interviews whenever the participants had the chance to meet with them.

69 For example, The Carter Center mission observers noted that one machine did not recognize the memory stick (external memory), which it needed to be opened. The memory stick was removed, re-inserted, and the machine re-initiated, upon which it recognized the memory stick and started up correctly.

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 selected machines, and from a special memory stick, a Linux operating system was booted, which included the CNE's 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 compared to the ones recorded during the source code audits. The result was both displayed on screen and printed out using the internal printer of the voting machine. On finding a positive match, an "OK" was printed next to each archive name. Generally, this process occurred without any major incident.[70]

Once all machines were operational, the voting process began. Operators performed the steps to begin voting (printing the diagnostic report and the zero tape) and began entering random votes into the machines, verifying that their choice was correctly represented on the paper receipts printed by the machines. The receipts were collected in special envelopes. Observations were recorded on a form, acta de auditoria pre-despacho (parte I: ingreso de votos), which was signed by all observers of the process. A total of 50 votes were entered for each voting machine.[71]

The operators proceeded to record the actual votes for each party/candidate on a second form, *acta de auditoria pre-despacho (parte II: planilla de conteo)*, which was also signed by all observers of the process. After voting was complete at a machine, if the time was already 4:00 p.m. or after, operators performed the procedure to finish voting and printed the *acta de escrutinio*, the official precinct tally record, which was placed in an envelope. If it was before 4:00 p.m., the operators waited until 4:00 p.m. and then commenced the closing procedure.

Under normal voting conditions, after printing the precinct tally, each machine would be directly connected to its respective medium of transmission. According to the procedures put into place for December 3 (election day), most machines (20,615 *mesas*) would be connected via fixed telephone lines; in some cases (7,681 *mesas*) a mobile phone was used for transmission via CDMA 1X; and in a small number of cases (4,035 *mesas*) where no communication was possible, the machine's memory stick (containing the votes) would be removed and physically transported to the nearest transmission center to transmit results from there to the tally center.

Due to the space restrictions in the audit hall (the tables where the voting takes place had no telephone lines) the operators proceeded to replicate the case of voting in remote places without connectivity. They removed the memory sticks from their machines and brought them to the audit hall's transmission center, which consisted of a table with a small number of special voting machines connected to a fixed telephone line.[72] These voting machines ran special software that only allowed transmission, not vote casting. This software was reportedly the same as that installed on the voting machines in the contingency transmission centers (CTCs) on election day.

70 The published audit procedure specified a final hash verification for these six machines after transmission had taken place, presumably to verify that no code had been altered during transmission to the tally server, as well as an in-depth hardware inspection of several machines chosen by the party representatives. Neither of these measures was observed by The Carter Center mission so we cannot confirm they took place. On the other hand, Carter Center mission observers noticed one case in which there seemed to be errors running the hash verification program. A technician spent some time troubleshooting until the program ran and successfully produced the hash which was printed and accepted as matching by the party representatives.

71 At a number of machines, the votes entered were not random, but rather entered following a pre-determined list of votes, which was agreed on with the political party representatives before-hand. These pre-determined lists of votes could contain a different number of votes (other than 50).

72 Another connection method that was used was a mobile phone connected via the serial port of a voting machine in the transmission center.

The technical personnel at the transmission center then proceeded to transmit the votes contained in the memory stick to the tallying server. The transmission report was included in an envelope together with the other minutes and documents.[73]

All of the envelopes with the minutes, as well as the memory sticks, were then submitted to the coordination table, where CNE staff, auditors, and observers compared the votes recorded in the machine-generated *acta de escrutinio* with the results recorded from the paper receipts. If no discrepancies were found, a final comparison result was printed and stored together with the envelopes and memory sticks. In case of discrepancies during counting, recounts were performed to correct possible human error. If errors persisted, a supervisor had to be consulted to resolve the situation. On the basis of what The Carter Center mission observed, there did not appear to be a defined process for handling machine-generated errors (for which this audit is meant to check), other than to "call the supervisor."

Finally, once the results had been transmitted and arrived at the tally server in the counting center, they were compared, via a secure (https) web interface querying the tally server's database, with the results of the manual count as recorded in the comparison report.

**Summary of Observations**

While the pre-dispatch audit generally proceeded smoothly, Carter Center mission observers noted the following issues:

- *A limited number of machines had their software hashes verified.* Of the 164 audited machines only six had the hashes of their voting software actually verified, suggesting that only these six machines can effectively be drawn upon to prove that the software as inspected, approved, and signed during the source code audits was installed and functioned correctly.
- *System date was not set to voting day. Time was forwarded to 3:00 p.m.* While the time on the machine was forwarded to 3:00 p.m., the machine's internal clock/calendar was not set to election day. Because the efficacy of such a test relies on the conditions of the election day being reproduced, both the date difference and the time forwarding procedure constitute important methodological limitations. Any advanced malignant code (if the system software were to contain any) would use a trigger mechanism specifically made to prevent it from being activated during a test situation. For example, it could be triggered by the election date, or by the internal clock in the machine. If such malignant code had been present on the machines during the test, it could have been programmed to activate some time after the planned opening time of polling stations (say 9:00 a.m.) and deactivate after noon (say at 2:00 p.m.). Since the machines skipped that time frame, and started testing only after 3:00 p.m. system time, as well as operating on November 26, instead of December 3, such a code would not have been triggered during testing, in contrast to voting day when it would have been triggered.
- *Not all of the machines were tested at the same time.* The fact that batches of voting machines were moved in and out of storage during the test instead of being set up all together at once and remaining in a controlled environment, unnecessarily increased audit time and reduced the quality of the testing environment by creating a high degree of personnel movement during the test. Considering the large investment that the CNE has made implementing an automated voting system, hiring a sufficient number of operators and having all of the required facilities available so that the selected machines could all be tested at once would seem a better option.

73 In one observed case, the connected voting machine correctly displayed, upon insertion of a memory stick, that that memory stick contained votes from a closed voting machine, which had not been transmitted yet. It proceeded to successfully transmit its minutes to the tallying server. Using a web interface to display real-time results from the tallying server (located at the CNE central office), it was verified that the data had been correctly transmitted. Upon trying to transmit the same data again, the tallying server accepted the communication, but did mark the received information as "already received."

- *A 50-vote limit was established.* As 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 "inventory of all machine parts," 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 "Parallel Vote" election day procedures, see Rezende (2004).

75 Colegio Nuestra Senora de la Consolación, in Caracas

machines, and that none of them had attended despite being informed. Polling officials argued that they did not receive any such invitation.

Trying to assuage concerns, the responsible *Plan República* officer intervened, stating that "no irregular things had happened" the day before, that he had "observed everything" and could "guarantee the correctness of the process." In the face of continued doubts on the part of some table members, he pointed out that "in any case, on the day of the elections the machines would print out a zero tape, which would be the final proof that no manipulation had taken place, or else it would show there." The table authorities appeared reassured by this and did not take any further actions in the presence of The Carter Center team. The confusion observed by The Carter Center mission suggests that table authorities, poll workers, machine operators, and *Plan República* officers in future elections would benefit from clearer guidance regarding the roles and responsibilities of polling staff during the rehearsal, as well as more clearly defined, and consistently articulated, chain-of-custody procedures.

Members of The Carter Center team visited several other polling places unannounced. Generally, observers found the polling place environment to be less confused than at that first polling station. While they did observe several instances of minor irregularities, such as broken tamper-evident seals, they were not considered to be of such severity that the integrity of the dry-run was undermined.

## Audits Performed During Election Day

After the polls closed on election day, and once the transmission of the results had finished, a drawing was carried out in all the polling centers to determine the tables where a hot audit or closing audit would be performed. The drawing was made based on a table prepared by the CNE (see Figure 6), again using the "pulling machine numbers from a hat" method.

| Number of machines in a polling center | Machines to be audited |
|---|---|
| 1 to 2 | 1 |
| 3 to 5 | 2 |
| 6 to 8 | 3 |
| 9 to 10 | 4 |
| More than 10 | 5 |

***Figure 6: Number of machines subject to a hot audit, per polling station***

Once the machines were selected, their corresponding paper slips were publicly counted by the table authorities. Both the total number of paper slips and the votes on each slip were recorded. The results of this process were then expressed in an official audit document, and included together with the other official documents for subsequent submission to the CNE.[76]

The defined hot audit procedure did not include any comparison between the results of this manual recount and the precinct tally result report printed by the voting machine. The procedure was only a transcription of the paper slip contents onto an official document, but without any comparisons. Despite this, in most of the voting centers observed by the Carter Center team, table authorities and witnesses informally and on their own initiative compared the manual count results to the printed precinct tally results report, performing what could be actually called a partial audit. However, there was no formal mechanism for this procedure, nor were there any documents on which to record the results or which described the procedures to follow should there be a discrepancy between the two sets of results.

The Carter Center mission is not aware of any case where, while following this procedure, local results (paper slips or printed precinct tally result report) were compared with results received at the central tally server on election day. This comparison was done the next day in the post-election audits.

76 This, while not exactly an "audit," is part of the basic set of fraud countermeasures as defined in Norden et al (2006) p. 26

## Observation in the Tally Center and in the CANTV Network Control Center

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 República* 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 a manual "pulling machine numbers from a hat" method similar to the one used during the machine production audit. While this did allow some degree of participant involvement in the audit process, it is doubtful that participants would have been able to detect any irregularities or non-sequential or missing numbers from a universe of over 10,000 numbers (one for each polling center) that they were asked to verify.

The audit was designed and organized by the Central University of Venezuela (UCV), who the CNE contracted for this purpose, and was carried out under controlled conditions in the AEROCAV assembly facility in *Filas de Mariche*. The audit teams were composed of CNE staff, mostly machine operators. Political party representatives were present during the process, as was the news media.

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

Following the procedures established for this dry-run, out of the one percent of polling centers selected at the CNE headquarters during election day, only those machines that had been hot-audited were audited again. Of the 175 selected machines, only 161 machines were actually audited because 14 machines were missing (replaced by "backup machines"). Another five machines could not be audited because the relevant documentation was missing.

During this audit, the paper slips corresponding to the audited machines were (again) counted. The results of this recount were compared to the hot audit record document generated by the table authorities on election day, to the machine's printed precinct tally result record, and to the results received in the central tally system. Due to its features, this procedure in principle conforms to the basic idea of a routine audit of voter-verified paper records at voting time. Such audits are being increasingly called for internationally and are legally required in some countries.[78]

The following steps were taken:

- Audit teams received boxes with the paper slips and the corresponding precinct tally record printouts.
- Teams counted out these slips and recorded the votes on minutes prepared for this audit, then compared them with the hot audit minutes completed by the corresponding table authorities at the end of election day and with the machine's printed precinct tally result record.
- If counts matched, the documents were brought to the coordination desk for later comparison with the central tally results. If counts didn't match, a recount was ordered. If the recount still showed discrepancy, it was assumed that some of the original paper ballots must be missing, and the audit teams started using the *chorizo* (the reprinted backup copies of the original paper slips) to correct the results from the original paper slips. The whole set of backup copies was not usually recounted, but 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 discrepancy would have to be recorded in the audit minutes, but no further consequences or procedures for such cases was specified.
- Ultimately, the paper count results were compared to the results recorded in the central tally database. For this purpose, a Microsoft Access application had been developed and installed on laptops in the audit hall. According to the UCV staff in charge, the results retrieved from the central tally database were sent by the CNE that day as a plain text file, via email, to a UCV staff person. The downloaded attachment was then fed into the Microsoft Access application as reference. According to interviews conducted on the spot, no party witnesses or observers were present during data retrieval, nor had the file been secured from modification using hashing or other security techniques.

Carter Center mission observers noted several cases of minor discrepancy; most of them caused by null-vote paper slips which had not been deposited in the ballot box (see usability section above). These discrepancies were corrected using the chorizo backup paper slip copies. During the comparison with the central tally results, several discrepancies occurred which were appropriately recorded in the minutes.

The degree of discrepancy was not large, ranging from 0 percent (Amazonas state) to a maximum of 1.62 percent (Trujillo state). The average was

78 In the USA, some form of routine auditing of voter-verified paper records is mandated in 13 states.

0.19 percent (57,505 votes counted, with 110 non-matching.)[79] Clear guidelines with regard to the acceptable margins of error did not appear to have been established in advance of the election. The Carter Center mission believes such guidelines would increase the overall transparency of the post-election audits in future elections.

The Carter Center observers noted that the purpose of the postelection audit, as a relevant and critical analytical tool to promote the integrity of the electoral process, did not appear clear to many of the auditing staff. The audit started late and auditors appeared to be suffering from audit fatigue.

Members of The Carter Center mission were informed by the CNE that non-aggregated audit records (per voting table, with transcribed election day comments as recorded by the table authorities) will be included in the final UCV audit report which may be requested once published.

**Formatting of Memory Sticks and Machines**

The day after the postelection audit, all memory sticks and the DOM memories should be formatted in order to prevent abuse of the data. The process of formatting should be observed by party witnesses and auditors.

Opposition representatives told Carter Center observers that the CNE had agreed to let opposition auditors audit certain "problem machines" before they were erased, including machines with broken seals (169 such cases were reported) and machines which had been located in polling centers where opposition witnesses had reported irregularities. All of those machines would be audited, regardless of whether their center had been selected for postelection auditing, or whether the machine itself had been selected for hot auditing. This audit should include verification of their installed software hashes to see if any software modification had taken place. The team of Carter Center observers left Caracas before this occurred.

**Summary of Recommendations**

- Negotiate complete audit procedures with political parties in advance of the audit process. This would allow auditors to adequately prepare for the audits and would promote greater transparency.
- During source code audits, accredited political party and observation group auditors should be given full and unrestricted access to the source code. This would allow a more meaningful audit process than the current audit review.
- Provide complete and detailed system documentation to accredited auditors in advance of the audit schedule so that they may adequately prepare.
- The sample size for the pre-dispatch and post-election audits should be determined according to appropriate statistical principles. This will allow the results to be extrapolated for the totality of voting machines.
- During the election day hot audit, a comparison of the paper slip count to the machine printed precinct tally result should be a mandatory part of the procedure. The audited paper slip results should also be analyzed by statistical procedures, with clear processes in place in case of discrepancy between the paper and electronic results.
- Allow the results of a paper ballot recount to form the basis of a legal challenge to the electronic election results.

79 Data obtained from observing computer screens during the audit.

# Conclusions and Recommendations

Due to its relatively small size and short duration, the Carter Center's specialized, technical mission did not produce a comprehensive evaluation of the integrity of the electronic voting system. Consequently, this report only has outlined the principal findings of the mission on those aspects of the electronic voting system that the observers were able to analyze and observe. Based on these findings, and in a spirit of cooperation with the National Election Commission (CNE) and the people of Venezuela, The Carter Center offers several recommendations that it hopes will contribute to the continued development of a robust electoral process in Venezuela.

## Voting Machine Design

In the polling places visited by the Carter Center team, a reasonable level of understanding of the technology among the electorate was observed, many of whom were able to cast their votes without incident. Given the relatively rapid and wide-scale introduction of the electronic machines, this is commendable. However, The Carter Center observers saw confusion among some voters, who claimed that they were unable to cast a null vote or who cast a null vote by accident. The Carter Center suggests that the CNE consider removing the paradigm break of the user interface process for the null vote. When casting a vote, the machine designates the touch pad as the place where a voter choice is made and the touch screen as the place where that choice is visually displayed and actively confirmed. The process for casting intentional null votes should be the same. The touch pad should contain a separate button for null vote, and that option should be displayed and confirmed on the touch screen, just as with regular votes.

The use of a voter verified paper trail and its placement in a ballot box after verifying it is a critical means of ensuring a transparent electronic election. The CNE should be commended for including this feature in the machine design. However, The Carter Center mission observers noted some cases in which voters unintentionally removed the ballot slip from the polling place. This was also observed in some of the postelection audits when minor discrepancies between the paper receipt count and the electronic results were discovered. The effectiveness of the paper trail as a tool for ensuring that the machines are accurately counting the votes of the electorate would be improved through better training of polling table members, who would then be able to minimize the risk of missing ballot slips. In addition, electoral authorities could consider a change to the system that would eliminate manual handling of the vote slips by, for instance, adopting technologies that only show the paper slip to the voter without allowing him or her to touch it (e.g., behind glass).

The current system does not establish a procedure for handling cases in which the voter alleges the paper-trail slip does not reflect his or her vote. Given that this situation undermines the main purpose of allowing voters to verify their votes, The Carter Center suggests that the CNE consider amending the system so that a voter can cancel or annul his or her vote if the printed receipt does not reflect the vote that was cast on the touch screen. Those procedures would allow the electronic vote to be deleted and the paper slip invalidated, either through physical destruction or overprinting with a cancellation notice.

The paper sheet that is placed over the electronic touch pad includes candidate photos in its design, allowing illiterate voters to cast their ballots

unassisted. This is an important means of protecting the universal human right to the secrecy of the vote. The paper slip, however, does not include this feature. The CNE could take further steps to protect this right by including candidate photos and party symbols on the paper slip. This would allow illiterate voters to confirm their own votes without assistance. Printers on both voting machine models allow a minimum of 200 dpi image resolution, which should be sufficient for a rudimentary image of both the candidate and the symbol.

Following CNE regulations, voters only have two periods of three minutes each to cast their votes. This restriction could limit the ability of voters to cast their ballots, which, in turn, may affect their exercise of the right to vote. Therefore, electoral authorities should reconsider the two-times/three-minutes policy currently in place. Voters should not lose the right to vote because they have difficulties understanding the voting technology in use. The Carter Center encourages the CNE to seek a balance between the need for implementing measures to improve the speed and efficiency of the electronic voting system with the protection of the citizen's individual right to vote.

## Security of the System

The Carter Center is pleased that the CNE has taken a number of significant measures to protect the electronic voting system from external attack, such as encryption of data using standard industry algorithms, and the implementation of sophisticated data randomization mechanisms. Equally commendable is the introduction of a number of procedural measures that are intended to prevent physical tampering with the machines and voting materials, such as the inclusion of a 32-digit, alphanumeric serial number on each printed ballot receipt. While this measure deters forgery of ballot receipts, the numbers as they currently exist are not machine readable, which could obstruct large-scale efforts to verify the authenticity of paper slips. Therefore, the CNE should consider making the paper ballot serial number machine readable (for example, by including a barcode). By doing so, the serial number becomes a functional security feature that allows the authenticity of the papers to be verified during a paper count with reasonable effort.

While the CNE has placed emphasis on technological security solutions, future elections would benefit from further physical security measures to secure the machines from unapproved access. Among other measures, The Carter Center believes that access to the machine, especially to its ports, should be made more difficult. The Center suggests that all non-essential ports (such as the Ethernet port) should have their physical wiring removed, rather than be deactivated through the use of software. Critical ports like the USB ports (which connect the machine to the memory stick) could be protected more efficiently against tampering through the use of tamper-evident seals which are systematically checked and whose violation automatically and bindingly leads to replacement of the voting machine concerned. Ideally, access to sensible system parts, such as the BIOS configuration menu, should be completely disabled. If this is not feasible, a clear and public policy on password access to the system is necessary, as is reliable access logging and the mandatory analysis of these access logs, with predefined consequences for unapproved access.

With regard to the chain of custody, the members of the Carter Center mission noted several instances in which the procedures put into place for this important aspect of the electoral process were not clearly understood or were not rigorously applied. Therefore, the Center believes the CNE should consider taking further steps to improve chain-of-custody procedures for the transportation and storage of the voting machines. Ideally, the responsibility for security during installation and storage would be shared between the CNE and civil society, rather than depending exclusively on the CNE and Plan Republica. For example, transportation of voting machine boxes, as well as official minutes and

documents, could be handled jointly with political party representatives.[80] 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 "many eyes" principle may be achieved.

The Carter Center considers that it would be equally beneficial to use a uniform type of tamper-evident tape across the whole electoral system. The tape should include anti-counterfeit features that are well publicized among all stakeholders so that irregularities can then be easily recognized. Responsibility for the chain of custody will then be broadened, increasing transparency and trust in the system.

The Carter Center mission observed that the CNE has gone to significant lengths to protect the system from external electronic attacks. Nevertheless, The Carter Center believes that it would also be useful to provide additional layers of security that will further protect the central tally system and other aspects of the electoral process from possible internal malicious exploitation. The Carter Center suggests that the CNE consider using an independent, third-party certificate authority to issue the certifications securing the communication between the voting machines and the tally instead of the CNE's own certificate authority. The use of an independent, external certificate authority would improve the security of data transmission while increasing the trust of non-CNE stakeholders in the electronic system and the CNE.

## Audit Scheme

The audit scheme of the Venezuelan electronic voting system includes a wide array of hardware and software tests designed to promote the integrity of the electoral process. Due to its broad, comprehensive character, this framework can become an important tool for ensuring that the electronic voting technologies work as specified and as intended. As noted in the report, an important feature of the audit process was the responsiveness and flexibility of the CNE to amend the audit process at the request of stakeholders once it was underway. While this was an important means for political parties and civil society organizations to play an active role in determining the course of the audit scheme, The Carter Center recommends that the CNE negotiate the audit procedures with political parties and civil society groups in advance of the audits. The details of these procedures should then be documented in writing, with the explicit agreement of the parties involved, and then made public without further change. This would allow auditors to adequately prepare, based on a fixed methodology, which would facilitate the structured observation of the audit process. It would also increase buy-in by the opposition parties because they would be more fully involved in the development of the audits.

The audit process itself would also benefit from the participation of a well-informed auditing team. For this purpose, the CNE should consider providing complete and detailed system documentation to the auditors of accredited political parties and electoral observation groups in advance of the audit schedule. The auditors would then be able to adequately prepare for this task, thoroughly analyze the system architecture, and identify security risks.

The Carter Center also suggests that during source code audits, the auditors of accredited political parties be given full and unrestricted access to the source code.[81] In addition, auditors should be able to apply

80 This is also recommended as a crucial security measure by Norton et al (2006) p. 77

81 Another model is to use open source code. The organizers of Australia's Capital Territory's 2001 electronic election have embraced the open source model and rejected closed, copyright protected solutions. The eVACS system was cooperatively developed by a private company and a public university. During the programming, the constantly evolving versions of the software were regularly posted on the internet, for anyone to download during the six months of development. Anyone could have full and free access to all the source code, could run it, compile it, test it, run special tools on it, etc. Software experts and interested amateurs from the Australian public helped evaluate the system and informed the development team of errors that they found. Several errors were found this way, including a fairly serious problem, reported by an academic at the Australian National University. The final version of the software, running under the open source operating system, Linux, was published under the General Public License (GPL), and has since been freely available to the public (Zetter 2003, ACT 2001)

appropriate audit tools during an adequate period before elections. This would allow a more meaningful audit than the current code review process.

The use of random sampling techniques helped the audit processes to increase their credibility. However, they were not consistently used throughout the process. The Carter Center suggests that the sample for the predispatch and postelection audits should be sized and selected using an appropriate statistical framework. This measure would help ensure that the results from the sample can be confidently extrapolated for the total number of the voting machines.

The CNE should also consider determining and publishing an error threshold for audits before the audits commence (following standard statistical methodology), especially for the audits that test system and data integrity. In the event that error threshold is exceeded, it should be concluded that the system malfunctioned and that the integrity of the process cannot be verified. The CNE should determine and publish, in advance of the elections, possible measures to address or resolve the situation. They may include a recount of paper slips, a larger scale system audit, or even a repetition of the elections, according to the size of the error encountered.

The implementation of a large-scale hot audit on election day by table authorities is a key measure to ensure the system's transparency. Public participation in vote counting is an important element that promotes confidence in the election process. For this, the CNE should be commended. Hot audits in future elections would be improved by making a comparison of the paper slip count result with the machine-printed precinct tally result a mandatory part of the hot audit procedure. The results should be recorded in the official audit documents.[82] Additionally, the audited paper slip results should be analyzed to determine possible statistical anomalies.[83] The CNE might consider adopting a statistically significant threshold for such discrepancies between paper and electronic results with discrepancies that exceed this threshold triggering a mandatory forensic investigation to identify the causes of that anomaly. The Carter Center also suggests that the CNE consider that the results of a paper slip count during the hot audit be able to form the basis of a legal challenge to electronic election results, where there is a significant discrepancy between the paper and electronic election results.[84]

In cases in which discrepancies between the paper slip count results and the electronic results become apparent, effective remedial measures might include:[85]

- Impounding and securing all machines where the paper and electronic results do not match;
- Conducting a public investigation of all machines with discrepancies with the objective of identifying evidence of possible manipulations of either paper or electronic results;
- If evidence of tampering is found, widening the investigation to include all machines where similar problems could have occurred;
- Identifying the total number of machines affected and analyzing (based on sound statistical measures) whether the manipulations were sufficient to have an impact on the election outcome;
- If the answer to the previous question is yes, the CNE should repeat the elections.

82 For example, in the U.S., as of January 2007, 13 states require both voter verified paper trail and manual audits, or a random sample of machines comparing paper with electronic results. Source: www.verifiedvoting.org.

83 This analysis would have the potential to produce evidence on tampering. See Norden (2006) P. 76

84 Simply having one set of records overrule the other rewards attacks on that result set. For example, if electronic results always overrule paper, an attacker might focus on changing these without trying to also falsify the paper record. If paper overrules electronic results, then potential attackers would need to focus their efforts on manipulating the paper results.

85 see Norden et al, (2006) pp. 74–75; 90-92

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.cev.ie/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.)

# Lessons for Observing Electronic Elections

In most electronic voting systems, and especially in a system as complex and highly automated as the one described here, the number of issues that can be observed visually is limited. Unlike the observation of traditional manual elections, an international observer or political party witness could stand right next to a voting machine in use, a telephone line transmitting election data, or a tally server doing its sums, and would still not be able to determine whether the computers are actually working according to their stated specifications and the expectations of the electorate. Voting machine user interface (UI) observation (looking at the screen to see if everything is ok) is inherently incapable of detecting intentional irregularities or fraud, since any attacker would try to ensure that his or her actions are hidden behind a smokescreen of apparently regular and correct system UI display. Electronic fraud, while it is happening, is practically invisible.

The observation of electronic elections by international organizations must therefore place emphasis on the observation of audit procedures and the design and implementation of chain-of-custody procedures, as well as an understanding of the system architecture and the legal and institutional framework. The presence of observers on election day, while still important, by itself is insufficient. Audit observations, and subsequent analysis of the audits' comprehensiveness and quality, may yield more meaningful results regarding the regularity of the elections than traditional visual observations during voting day. This is especially true if the involvement of the opposition and civil society in the design and implementation of the electronic voting system is limited—as is the case in Venezuela. In these cases, the audits become the principal means for all sectors to evaluate whether or not the electronic voting system has performed correctly, or has suffered from irregularities. The burden of fostering trust in the electoral results, in this scenario, lies almost entirely on the audit process.

On the observation methodology for electronic elections, much work remains to be done. The principal challenges lie in the lack of consistency of the technological solutions between various countries and the complexity of these systems as compared to traditional manual voting processes. Audit schemes also vary widely. It is no easy task to develop a unifying methodology that is applicable to all systems and audit schemes, but still streamlined enough for practical use during an observation mission.

Nonetheless, there are best practices for which an observer can check. For source code audits, this would be free, complete, and early access for accredited political parties to the totality of the system's source code. For parallel testing type audits (black-box/data tests), it would be the application of statistically sound methods to determine sample sizes, the complete randomness of selection of those sample machines, and re-creation of the exact same voting conditions as occur in polling places on election day. For paper-trail hot audits, it would be, again, sample size and the use of reliable methods to compare the paper trail with the centrally received electronic results. Finally, and here the election day observation is still very relevant, it would require an effective chain of custody, with responsibility shared by all political stakeholders and rigorously secured against violation, to form the backbone of electronic security. Effective security policies regarding personnel access and password knowledge are also necessary for electronic security to be meaningful.

Beyond that, the general degree of centralization and unilateralism of decision making versus

participatory approaches involving all stakeholders is an important indicator of system reliability regardless of the details of the technological solution employed. Checks and balances in no way become irrelevant in the age of computerized voting.

The continued development of a checklist of "questions to be asked"—many of which will be answered before, not on, election day through the study of documents and interviews—is the next step toward a more uniform methodology of observing electronic elections.

# 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/.

Brunazo, A. (2004). O Voto de Cabresto Póst Moderno. http://www.votoseguro.org.

Caltech-MIT (2001). Voting - What Is, What Could Be. The CALTECH-MIT VOTING TECHNOLOGY PROJECT .http://vote.caltech.edu.

Calvo, E.: Escolar, M.; Pomares, J. (2007). "Split Ticket incentives under alternative e-voting advices: experimental evidence on information effects in multiparty elections." American Journal of Political Science. (forthcoming)

CNE (2006c) Manual Operativo para Miembros. Secretaria o Secretario de Mesa Electoral. Elección Presidencial 2006.pdf.

CNE (2006d) Instructivo dirigido a los Efectivos del Plan República. Elección Presidencial 2006. pdf.

CNE (2006a) Porqué su voto es secreto. Elección Presidencial 2006.pdf.

CNE (2006b) Manual del operador de máquina. Elección Presidencial 2006. pdf.

CNE (2006e)Tríptico OMV Elección V7. (13112006) Elección Presidencial 2006. pdf.

CNE (2006f) Official Minutes of the Audits of the Venezuela Presidential Elections, Presidential Elections 2006. (set of photocopies)

Elklit, J. y Reynolds, A. (2002). "The impact of election administration on the legitimacy of emerging democracies: a new comparative politics research agenda." en: Commonwealth and Comparative Politics. Vol 40. No. 2: 86-119.

Gobierno Ciudad Autónoma de Buenos Aires (2005) 2005. E-voting Pilot Project. First Evaluation Report. Executive Summary. Buenos Aires.

Hartlyn, J.; McCoy, J. (2006). "Observer paradoxes: How to Assess Electoral Manipulation," in: The Dynamics of Electoral Authoritarianism. (A. Schedler, ed.). Boulder (Co), Lynne Rienner, Pub.

Hartlyn, J; McCoy, J; Mustillo, Thomas (forthcoming 2008). "Explaining the Quality of Elections in Latin America." Comparative Political Studies.

Leohucq, F. (2003). "Electoral Fraud: Causes, Types and Consequences, Annual Review of Political Science 5: 233-256

López Pintor, R. (2000). Electoral Management Bodies as Institutions of Governance. New York. United Nations Development Program.

Massicotte, L.; Blais, A.; Yoshinaka, A. (2006). Establishing the Rules of the Game. Elections Laws in Democracies. Toronto. University of Toronto Press.

Mercuri, R. (2002). A Better Ballot Box? New electronic voting systems pose risks as well as solutions. IEEE Spectrum Magazine. October 2002. Available at http://www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html.

Neumann, P. (1993). Security Criteria for Electronic Voting Proceedings of the 16th National Computer Security Conference Baltimore. Maryland. September 20-23. http://www.csl.sri.com/users/neumann/ncs93.html.

Neumann, P. (1995). Computer Related Risks, Addison-Wesley, http://www.csl.sri.com/neumann.

Norden et al. (2006). The Machinery of Democracy: Protecting Elections in an Electronic World. Voting Rights & Elections Series. Brennan Center for Justice at NYU School of Law. 2006.

RABA (2004). Trusted Agent Report—Diebold AccuVote-TS Voting System. http://www.raba.com/press/TA_Report_AccuVote.pdf.

Rezende, P. (2004). Electronic Voting Systems: Is Brazil ahead of its time?, CryptoBytes Magazine. (RSA Laboratories). Volume 7. No. 2. Fall 2004.

Schedler, A. (1998). "Delegation without discretion. The Bureaucratization of Electoral Administration in Mexico." Paper presented at the: XXI Congreso Internancional de Latin American Studies Association (LASA). Chicago. September 24-26.

Smartmatic S.A. (2006). Smartmatic Automated Election Systems—SAES_v3.2 101006.pdf.

Smartmatic, S.A. (2006a) SAES, Carter Centre.pdf.

Tadayoshi, Stubblefield, Rubin, Wallach (2003). Analysis of an Electronic Voting System, Johns Hopkins University Information Security Institute. Technical Report TR-2003-19. http://avirubin.com/vote.pdf.

Thompson, K. (1984). Reflections on Trusting Trust. Communication of the ACM. Vol. 27. No. 8. August 1984. pp. 761-763. http://http://www.acm.org/classics/sep95/.

Zetter, K. (2003). Aussies Do It Right: E-Voting. Wired Online News. November 2003. http://www.wired.com/news/ebiz/0,1272,61045,00.html?tw=wn_story_page_prev2.

# Appendix A
# Carter Center Observation Methodology

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 centers after the manual transportation from polling stations.

This variable has a potential impact on the closing part of the process.

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. "Ruling party" 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

According to the official minutes, source code audits took place between Oct. 16 and Oct. 31, 2006. Carter Center observers were not personally present during any of these audits.

**Oct. 16:**

The Carter Center did not receive official minutes for the procedures on Oct.16. According to a brief GST audit report, on that day hashes were generated of the source code files to be audited in the upcoming audit sessions. Also, a timeline for these sessions was agreed upon.

**Oct. 17:**

According to the official minutes the following happened:

- A "controlled operating environment" was created by installing the hash-verified image of Windows XP Embedded that was created during the previous hardware audits on a PC.
- The source code of the "applications for the Presidential Elections 2006" was copied onto that PC.
- Hashes of these source code files were created and compared to the ones created on Oct. 16 to ensure that the same source code would be audited.
- The following applications were compiled: election; InstallSAES; CTS; CFEncryptor; BallotProduction; SAESDataUtil.
- The applications were protected using a multipart password (the parts of which are known only to the respective participants—one part to the political parties, one to the CNE, and one to the vendor Smartmatic). This was done using the application "GenKeyAndProtect," 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 "Plantilla_Hashes_Binarios_y_Fuentes.txt" 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 representatives' 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 "did not have network card drivers," 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:**

According to the official minutes the following happened:

Revision of memory stick replacement mechanism, and revision of voting machine replacement mechanism.

***Notes and Observations:***

No further detail was included in the official minutes.

**Oct. 26:**

According to the official minutes two new audit procedures were implemented that had been specifically requested by the party representatives. At their request these procedures were included in the audit process:[87]

- Both a 3000 and a 3300 model were booted from a Linux memory stick and a script run called "revisar-hardware.sh" which detects all physical components of the voting machine.
- Using the Process Explorer tool, it was identified which dll's were used by the Election application. Of the 89 dll's found, 20 were selected as important and hash values generated from all. The hash values were stored.

**Oct. 31:**

The last audit of the voting machine software took place. According to the official minutes the following happened:

- A one percent sample of all the voting machine configuration files (in clear text) was taken.[88]
- The sample files were encrypted using the CFEncrypter application.[89]

87 This is an example of the aforementioned ad-hoc changes to the process.

88 It is assumed that these configuration files are the ones stored on the memory stick. Upon inserting the stick into a "blank" voting machine, it copies the configuration files to that machine and configures it permanently for that specific polling station and table.

89 This is the same application that the voting machine uses to handle its encrypted configuration files. Its authenticity was verified via hash.

- 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 "was verified in all the burn stations."[90]

## Central Tally 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 functional modules 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 "entire 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 days' proceedings.

92 The table is too long to be represented here.

Various version updates of software under review (database handler module and "transmitted tally" report module),[93] further revision of *actas por boletin* report module, and a revision of the EMS module that generates the voting machine certifications on election day.

***Notes and Observations:***

The version updates are not further specified, nor are any consequences to the audit process that may have resulted from these updates. These minutes bear a remark on the front page, noting that three pages of so-far unanswered questions had been submitted by the opposition representative as part of the minutes. The annex was not attached to The Carter Center copy obtained from the CNE. One of the opposition auditors informed The Carter Center that during some of the source code audit sessions, "appendix sheets" had been submitted as part of the minutes, detailing pending questions and informal agreements made during the audit sessions.[94]

**Nov. 7:**

According to the official minutes the following happened:

Further revision of the EMS module that generates the voting machine certifications on election day, continued revision of the database structure, and revision of the WEB.XML file of the JBoss application server.

***Notes and Observations:***

These minutes bear a remark on the front page, noting that one page of so-far unanswered questions had been submitted by the opposition representative as part of the minutes. This appendix is missing from the CNE-issued copy of the minutes.

**Nov. 8:**

According to the official minutes the following happened:

- Using a tool called JARSIGNER, hash values of the JAR files of the REIS and REIS listener (receiver) components were generated (MD5) and recorded.
- A requirement was made by the political parties to obtain hashes of the final configuration files of the JBoss application server and database objects. It was agreed to plan a date and time so that the definitive files, as will be used for the election, can be hashed.

**Nov. 21:**

According to the official minutes a special audit session was held in order to review changes to the source code in the modules REIS and REIS listener.[95] The resources of concern were "Error—messages. properties" and "language-ve.properties." The changed files were newly hashed using JARSIGNER, and the hash values recorded.

**Nov. 30:**

Two audit sessions took place, organized in response to the requirement of generating hashes of the final configuration files (see Nov. 8). The morning session took place in the main data center of the CNE (CNT1). According to the official minutes hashes of the configuration files of the following components were generated and recorded: complete tally system (REIS, REIS listener, Database handler) and the database itself.

The afternoon session took place in the contingency data center of the CNE (CNT2). According to the official minutes, the same hashes were generated and handed over to party representatives, and a review of differences and similarities between CNT1 and CNT2 (and the hashes of their configuration files) took place.

***Notes and Observations:***

Carter Center observers were not informed about this set of audits.

93 Details of these "updates" are not clear from the minutes.

94 Mr. Fidel Gil.

95 The reasons for these changes are not stated. We assume that development and bug fixing of the tally center software continued until a few days before election day, making source code modifications necessary.

## Machine Production Audit

| | |
|---|---|
| **Date of Observation** | Dec. 12, 2006 |
| **Carter Center Observer** | Ingo Boltz |
| **Place of Audit** | *Filas de Mariche* — Voting machine assembly facility of AEROCAV, guarded by *Plan República* military personnel |
| **Objective of Audit** | Select a random sample of 0.5 percent of all the voting machines prepared in the assembly facility of AEROCAV, seal them, and store them for the pre-dispatch audit on Sunday, Nov. 26, 2006. |
| **Organizations Taking Part in Audit** | *Comando Miranda, Comando Rosales, Universidad Central de Venezuela*, CNE (group called "the auditors" below) |
| **Notes** | According to Sergio Rivas of the *Universidad Central de Venezuela*, this audit took place on each day of production/assembly of the machines, beginning Nov. 1 and ending Nov. 23. Each day, 0.5 percent of the day's production was selected, sealed, and stored for later auditing. |

**Description of Procedure and Observations**

1. A worker from the plant assembly personnel presented a list of machines produced since the last production audit took place (the previous day). The list contains three IDs:

   ID1: A running unique ID number of the machine. This number is principally used for identifying the machine for the audit, and according to Rivas, is assigned by the UCV.

   ID2: Another unique ID number ("CVA"), containing in a number code the exact future geographic location of the machine (State, municipality, *Parroquia*, voting center, *Mesa*, and *Tomo*). This information is also spelled out in writing in the list.

   ID3: Another serial number for each machine. According to Rivas this number is used mainly in shipping logistics of AEROCAV. (It was not possible to establish whether this number is physically carved into the voting machine casing or simply assigned.)

2. The auditors verified that the running numbering (ID1) was correct, comparing the number produced since the last audit with the running numbers of the list.

3. The auditors calculated that 0.5 percent of that production equals 1.91 machines. Therefore, two machines would be picked for the sample.

4. The auditors placed paper slips, each containing one of the numbers from #31990 to #32371, in an open cardboard box. The representatives from the comandos mixed the slips.

5. The party representatives randomly chose, without looking into the box, one of the paper slips. The slips chosen today were #32371 and #32135.

6. This result was recorded in minutes by Rivas and signed by the auditors. These minutes are for use of the Central University of Venezuela; the CNE maintains the official minutes. The minutes, an envelope, with the remaining paper slips inside, and the selected slips glued to the envelope were stored by Rivas for the university records.

7. A member of the facility staff was asked to "go find and prepare these two machines for the sealing." The auditors did not personally accompany the facility staff member to ensure themselves of the process of taking these two machines from the production line.

8. After an estimated period of about 15 to 20 minutes, the facility staff returned, advising that the machines were ready.

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 República* 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 machines' (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 agreed that these were the correct machines, wrapped the whole pallet in plastic foil, and attached (using yellow tape) five sheets of paper with details of the day's audit and the signatures of the auditors, one to each side of the wrapped "package" except the lower side that rested on the pallet, which remained without sealing.

13. The auditors viewed how a forklift took the pallet and placed it on high storage in a rack in the assembly area, where other wrapped and sealed pallets from previous days' audits were visible.

14. It was said that this was the last audit of its kind because production had finished. Workers were mostly preparing backup machines, which were prepared to replace failing machines on voting day. On a regular day, production would average 1,500 units. Today, only the mentioned 382 units had been produced. The backup machines were not included in the number from which the auditors chose their sample two machines—they only chose from standard machines to be dispatched to voting centers.

15. The auditors left the production hall (with another metal detector check at the exit) and returned to the audit office.

16. Meanwhile, in the audit office, a CNE official had prepared the official CNE minutes, which were read and signed by all auditors.

17. The auditors left the facility.

According to a short interview conducted after the audit with Leonardo Hernandez, director general of information technology of the CNE, the machines that are removed, sealed, and stored to form the sample are replaced after the audit with identical clones and shipped to their planned location. These clones are created by programming a blank machine with the exact same configuration and geographic information as the machines that had been removed for sampling. It was not inquired how long the process of cloning takes.

***Comments:***

There was no doubt that the auditors chose two machines at random, even though the statistical rigor of the methodology was very limited. There were, however, two issues that caused doubts.

First, the auditors did not personally supervise the retrieval of their chosen machines. According to Rivas, in previous elections, following then-valid audit procedures, the auditors did pick machine numbers, personally enter the production facility, found the machines with the correct numbers, and supervised their removal from the production facility to the place where they were sealed by the auditors. However, due to the then-large number of auditors this created confusion in the facility and the process was slow. Therefore at the beginning of this election's set of audits (Nov. 1) the auditors agreed to change the procedure and trust plant staff with the tasks of searching for the machines and placing them on the pallet where their boxes would later be inspected and sealed.

When inquired whether the lack of personal supervision didn't mean that the machines chosen

at random could be switched for others during the unsupervised "searching and preparing of the sample machines" 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 "hot swapping" 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 plastic wrap that covers the whole "package," it may be possible to make a swap of machines later, at a more convenient moment (e.g., with plant staff absent) and with more time to prepare the clone machines.

In the case of the machines selected, the unsealed lower side of the two cardboard boxes could possibly have been opened and machines replaced without violating the seals.

In the case of the majority of the other pallets with the previously selected and sealed machines (which resulted from previous audits and were already on high storage when we observed), a violation of the seals is more difficult because they were inside their solid hard cases. In order to change machines it would be necessary to remove the plastic wrap (including the seals applied on top of the plastic wrap) without breaking it, switch the boxes with other boxes, and re-apply the plastic with the seals intact on top of the new boxes.

Both swapping schemes would be much harder to implement if the serial number of each machine (ID3) was physically engraved into each voting machine and was unique. If so, and during the pre-dispatch audit the serial number as noted in the minutes was compared to the serial number of the voting machine audited, a switching operation would require physically forging a serial number of the machine. Furthermore, two machines with identical serial numbers would exist (one in the audit sample, one in the field) that would also have to be covered up.

## 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 CNE's virtual private network, (provided by CANTV) as it developed on election day.<br><br>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:**

The control center is a room with restricted access inside the CANTV facility with a number of monitors for supervising the CANTV network's functions. It is not specifically dedicated to CNE operations; it is used to control the whole of CANTV's network operations.

During the observation, two CANTV employees were performing regular (non-CNE) tasks there, while four others were supervising activity in the virtual private network (VPN) that CANTV provided specifically for the CNE.

The main observation screen (projected to a back wall) contained the following four windows:

**1. Network Traffic per Router:** Traffic-over-time graphs for each of the VPN's principal router, with near-real-time (5 minute refresh) information on current traffic (bandwidth used) both into and out of the router. With all routers there was a principal router (1) and a contingency router (2).

Routers displayed were:

- CNE 1 & 2: principal router where all traffic to and from CNE converged
- Fixed Line Traffic 1 & 2: router receiving traffic from voting machines transmitting using fixed phone lines
- MOVINET Mobile Traffic 1 & 2: router receiving traffic from voting machines transmitting using mobile phones
- REDCOM Satellite Traffic 1 & 2: router receiving traffic from CTC transmission center using satellite
- Regional Election Authority Centers: one for each state

**2. RAS Statistics:** Number of modems in use at given time in different regional RAS.

**3. Statistics of number of tunnels and sessions in use at given moment**

**4. Snapshot of Voting Machines Communicating with CNE Router at Given Moment** (see Figure B.1)

| Username of machine | IP assigned | Idle time in seconds |
|---|---|---|
| "log_Machinecode@cnep2006.gob.ve" | … | 23 |
| "log_Machinecode@cnep2006.gob.ve" | … | 12 |

***Figure B.1: Example of how list of voting machines in communication with CNE router was displayed.***

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, beginning with about 10 sessions and 37.4 kb/s total traffic at the CNE router (inbound)
- At about 16:45, 40 sessions, 62.6 kb/s total traffic CNE (inbound)
- At about 17:00, 60 sessions, 130 kb/s total traffic CNE (inbound), 2 tunnels
- At about 17:20, 136 sessions, 381 kb/s total traffic CNE (inbound); 157 total traffic CNE (outbound); 4 tunnels
- At about 17:25, 232 sessions, 465.9 kb/s total traffic CNE (inbound); 192.2 kb/s total traffic CNE (outbound); 5 tunnels
- At about 17:50, 330 sessions, 767.3 kb/s total traffic CNE (inbound); 313.8 kb/s total traffic CNE (outbound); 5 tunnels
- At about 18:15, 368 sessions, 853.7 kb/s total traffic CNE (inbound); 335.5 kb/s total traffic CNE (outbound); 5 tunnels

***Premature End of Observation***

Shortly after taking the last data point, the observer noticed on the traffic graph that traffic seemed to level off and even fall slightly. He left the restricted MiniCore area to use the restroom, and when he returned he was not permitted re-entry; officials did not say why. **Therefore, the observation could not be completed.**

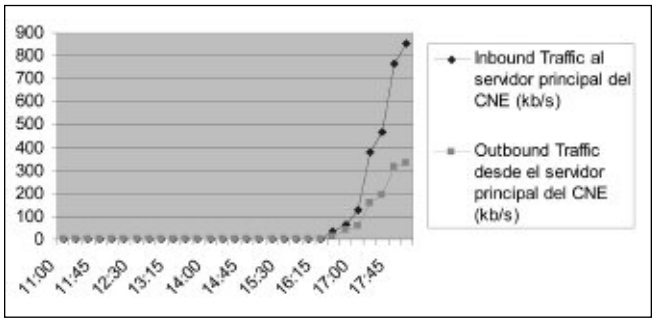


***Figure B.2: CNE Network Traffic Observation.*** *Minimal traffic (about 1kb/s) was recorded on the CNE principal router between 12:00 and 16:00. However, no tunnels were open and no sessions were established. CANTV staff commented that they were not sure what that network traffic was, that they had sent a report to the CNE, and that the issue was going to be investigated.*

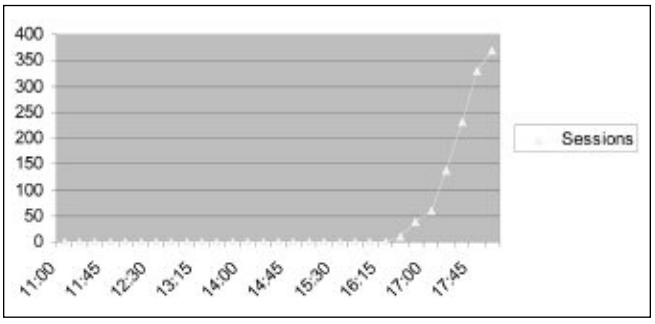


***Figure B.3: CNE Network Traffic Observation.***

# Appendix C
# Carter Center Statement About the Venezuelan Elections


## Carter Center Announces Technical Mission to Observe the Venezuelan Elections

**Nov. 16, 2006**

For Immediate Release

**Contact:**
In Caracas, Josefina Blanco 58-416-614-2948
In Atlanta, Deborah Hakes 404-420-5124

In response to an invitation from the Venezuelan National Electoral Council, The Carter Center will organize a specialized, limited technical mission for the Dec. 3, 2006, presidential elections. In accordance with the Declaration of Principles for International Election Observation, signed by over 20 international organizations at the United Nations in October 2005, election observation missions may be either comprehensive missions intended to evaluate an electoral process in its totality, or they may be specialized, limited missions to focus on particular aspects of the process.

In this case, The Carter Center technical mission will observe the use of the automated voting technology in Venezuela through participation in some audits and simulations sponsored by the CNE. The mission will be composed of two medium-term experts in Caracas from Nov. 20 – Dec. 5, and a short-term team of four-to-six additional experts during the days surrounding Dec. 3. Because of its short duration and limited focus, the specialized technical mission will not produce a comprehensive evaluation or assessment of the integrity of the automated voting system in Venezuela. Nor will the mission issue a public statement on election day or its immediate aftermath. However, the mission will produce a report after the elections summarizing its findings on the components and the functioning of the Venezuelan system in a comparative analysis with other automated voting systems in selected countries, and making recommendations on this basis.

The mission will also contribute to a larger effort of The Carter Center, in cooperation with other major international organizations, to develop and update methodologies for observing and evaluating automated voting systems globally.

# Appendix D
# Baseline Survey for Electronic Voting Systems

**Draft**

***May 2007***

The information gathered by answering these questions should create a comprehensive picture of the voting system in use and thus allow a more full assessment of its use.

Information should be gathered through review of appropriate legislation, decrees, bylaws and rules, and interviews with election administration officials, technical and legal experts, representatives of political parties, and domestic observation and civil society organizations.

Any supporting documentation should be retained including the elections law, certification procedures, standards against which the technology is measured, reports on past processes, and so forth. Be sure to include details about how, where, and when the information was obtained, and, particularly in the case of interviews, the name, title, and affiliation of the source of the data. This process likely will occur over a number of weeks in the months leading to election day.

After collecting as much data as possible regarding the use of the electronic voting system, a synopsis of your findings will be written. This synopsis will provide an overview of the system that can be used by other observers as a point of reference. In addition, data collected will be used to modify more generic election day and other checklists to capture information on the actual functioning of the system.

## Technology Overview

1. Which types of voting system technology are used?
   a. Direct recording equipment (DRE)
   b. Precinct count optical scan equipment
   c. Central count optical scan equipment
   d. Lever machines
   e. Electronic poll book
   f. Ballot marking devices

2. Are these technologies used throughout the country? If no, please attach maps indicating where different technologies are used.

3. What version or versions of all hardware, software, and firmware components are deployed in the voting system technologies, including but not limited to any version of the following:
   a. Smart card devices
   b. Firmware used in touch screens
   c. Vote counting server
   d. Other (please describe)

Note. The Carter Center would like to acknowledge the Verified Voting Foundation (www.verifiedvoting.org), the work of which informed the Center's methodology.

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

### Voter Verified Paper Trails (VVPT)

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?

### Certification

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?

### Acceptance Testing

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?

### 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. 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?

### Security and Integrity of the System

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.

### Software

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.

## Central Tabulating Computer

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.

### 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 access to that database throughout the electoral process?

105. Is there an independent review of the electronic poll book database? If so, by whom?

106. Is the voter roll database connected to any other databases (e.g., databases of biometric data) ?

### Ballot Building

107. Who is responsible for building the electronic ballots?

108. Is there independent review of the database from which the ballot is built?

109. Are there official guidelines or regulations for ballot building? Please attach if available.

110. What is the process for building ballots? Please provide a detailed description of this process.

111. Does the electronic ballot replicate the paper ballot in layout, candidate order, and design?

## Public Confidence in Electronic Voting Technologies

112. Are civil society organizations reporting on issues related to electronic voting? If so, please attach any pertinent documentation.

113. Are the media reporting on issues related to electronic voting? If so, please provide a sample of relevant stories.

114. Are simulations of the opening, voting, closing, and counting procedures provided and open to the public? If so, please provide further information about location, timing, and attendance of the simulations.

115. Are there public information drives about the use of electronic voting?

116. Have voters, political party agents, domestic observers, or others received training on the electronic system in use?

117. Have any opinion polls been conducted related to the use of electronic election technology? If so, please attach any available results reports.

118. In your opinion, does there appear to be a sense of concern among the general public about the transparency of electronic voting systems? If so, has the state responded to these concerns? Please explain.

119. Were political parties consulted during the technology procurement process?

120. Are there any political parties or individual candidates who are campaigning on issues related to the use of electronic voting? Please provide further details.

## 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
    f. Vote counting and tabulation procedures
    g. Storage and transportation of polling place results

127. Can a voter spoil his or her ballot? If so, how? Please describe how a vote can be spoiled and what happens to spoiled ballots.

128. Can a voter cancel his or her vote prior to casting the ballot? If yes, what is the process of cancellation?

## Contingency Planning

129. Does the law or official rules and regulations require the following?

    a. Contingency plans are in place in case of equipment failure.

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?

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. Have past election results been disputed because of the use of electronic voting technologies? If so, please attach a summary of the complaint, its resolution, and any related procedural or legislative changes regarding the use of electronic voting technologies that followed.

# Appendix E
# Poll Opening Observation Form
***Venezuela 2006***

**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? _____

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. If yes, who maintains the documentation?

_____

_____

## Poll Opening

| | Direct Observation | | Reported to Our Observers | | Not Observed or Not Applicable | |
|---|---|---|---|---|---|---|
| 9. Are electronic voting machines positioned: | | | | | | |
| a. With enough distance between them, at such an angle, and with shields to ensure privacy? | Yes | No | Yes | No | N/O | N/A |
| b. To plug into an electrical outlet?* | Yes | No | Yes | No | N/O | N/A |
| 10. Are the polling officials and support technicians properly accredited and identified?* | Yes | No | Yes | No | N/O | N/A |
| 11. Did the polling officials perform diagnostics and print the diagnostic report for all machines?* | Yes | No | Yes | No | N/O | N/A |
| 12. Was the setup of the machines completed without problems?* (If yes, skip to question 13) | Yes | No | Yes | No | N/O | N/A |
| a. If no, could the polling station technicians resolve the problem within the specified 30 minutes? | Yes | No | Yes | No | N/O | N/A |
| b. If technicians could not resolve the problem, was the machine replaced with another machine within the maximum of 120 minutes (counting from occurrence of the problem)? | Yes | No | Yes | No | N/O | N/A |

| | 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 standard release button or the standard ballot tablet)? | Yes | No | Yes | No | N/O | N/A |
| 14. Before voting began, did each machine produce a zero tape? * (*Acta cero*) | Yes | No | Yes | No | N/O | N/A |
| 15. Did the polling officials store the diagnostic reports and the zero tapes in the supplied envelopes? | Yes | No | Yes | No | N/O | N/A |
| 16. Did polling officials log the identification number of each machine as it was opened and prepared for the election?* | Yes | No | Yes | No | N/O | N/A |
| 17. Did you observe the official tamper-proof tape that sealed the case in which the voting machines arrived?* | Yes | No | Yes | No | N/O | N/A |
| 18. Did the case contain all the required machine components?* | Yes | No | Yes | No | N/O | N/A |
| 19. Did you observe tamper-proof seals or tape covering the ports of the machines prior to their setup?* | Yes | No | Yes | No | N/O | N/A |
| 20. Did polling staff receive all equipment needed?* | Yes | No | Yes | No | N/O | N/A |
| 21. If applicable, did polling staff receive an adequate number of paper ballots in case of failure of the machines?* | Yes | No | Yes | No | N/O | N/A |
| 22. Are the machines set up so as to be accessible to disabled voters who may need special equipment, be in a wheelchair, or have other restrictions on their movement? | Yes | No | Yes | No | N/O | N/A |
| 23. Did polls open on time? | Yes | No | Yes | No | N/O | N/A |

## 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 used at the polling station? (Fingerprint system—SAV/*Captahuellas*) | Yes | No | Yes | No | N/O | N/A |
| 25. Was the fingerprint system set up without problems?* | Yes | No | Yes | No | N/O | N/A |

Comments

# Appendix F
# Election Day Observation Form
***Venezuela 2006***

**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? _____

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. If yes, who maintains the documentation?

_____

_____

## After Polls Open

| | | Direct Observation | | Reported to Our Observers | | Not Observed or Not Applicable | |
|---|---|---|---|---|---|---|---|
| 9. | Do electronic ballots seem complete and contain all appropriate candidates and races?* | Yes | No | Yes | No | N/O | N/A |
| 10. | Do the screens appear to be properly calibrated?* | Yes | No | Yes | No | N/O | N/A |
| 11. | Do electronic ballots appear to be operating properly?* | Yes | No | Yes | No | N/O | N/A |
| 12. | Does the ballot touchpad appear to be properly calibrated?* | Yes | No | Yes | No | N/O | N/A |
| 13. | Are voters on electronic systems made aware by the machine that they might be undervoting?* | Yes | No | Yes | No | N/O | N/A |
| 14. | Do voters seem to find the instructions for casting a ballot clear?* | Yes | No | Yes | No | N/O | N/A |
| 15. | Do accessibility devices appear to be working properly?* | Yes | No | Yes | No | N/O | N/A |
| 16. | Do election officials keep a running tally on a regular basis through the day to ensure the number of votes on the machine is consistent with the number of people who have voted? | Yes | No | Yes | No | N/O | N/A |

| | 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

# Appendix G
# Poll Closing Observation Form
***Venezuela 2006***

**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. 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?
   _____
   _____

7. Who delivered the equipment to the polling station?
   _____
   _____

8. Was this chain of custody documented? Yes No

9. If yes, who maintains the documentation?
   _____
   _____

## Poll Closing

| | Direct Observation | | Reported to Our Observers | | Not Observed or Not Applicable | |
|---|---|---|---|---|---|---|
| 10. Once voting has finished for the day, do poll workers follow procedures to complete the process and close the polls?* | Yes | No | Yes | No | N/O | N/A |
| 11. Is the memory card containing the voted ballots removed from the port? | Yes | No | Yes | No | N/O | N/A |
| 12. Were the polling place totals successfully printed?* | Yes | No | Yes | No | N/O | N/A |
| 13. If not, were the proper contingency procedures followed?* | Yes | No | Yes | No | N/O | N/A |
| 14. Do polling officials print polling place totals before sending any electronic communications out of the polling place via connection to a network? | Yes | No | Yes | No | N/O | N/A |

| | Direct Observation | | Reported to Our Observers | | Not Observed or Not Applicable | |
|---|---|---|---|---|---|---|
| 15. Was the transmission method as originally planned for this polling station used? | Yes | No | Yes | No | N/O | N/A |
| 16. Did the transmission to the central tally server complete?* | Yes | No | Yes | No | N/O | N/A |
| 17. Was transmission successful at first attempt?* | Yes | No | Yes | No | N/O | N/A |
| 18. If transmission was not performed locally and the memory sticks were transported to the nearest transmission center, were the prescribed security measures followed?* | Yes | No | Yes | No | N/O | N/A |
| 19. Is a copy of the printed polling place totals available for public review at the end of the day?* | Yes | No | Yes | No | N/O | N/A |
| 20. Were copies of the electronic tallies printed for all party observers (nine in total)? | Yes | No | Yes | No | N/O | N/A |
| 21. Was public access to the audit process free from intervention by the military or other government authority?* | Yes | No | Yes | No | N/O | N/A |
| 22. Do election officials appear to understand and adhere to the required procedures?* | Yes | No | Yes | No | N/O | N/A |
| 23. Were there any complaints arising from the use of election equipment? If so, please provide details, including their resolution. | Yes | No | Yes | No | N/O | N/A |

## Election Day Auditing

24. Was a hot audit conducted? Yes No

25. Who conducted the hot audit?

_____

_____

_____

26. How many machines in your polling place were audited?

_____

_____

_____

27. How were the machines selected to be audited?

_____
_____
_____
_____

28. If an unofficial comparison of the count of the paper receipts with the electronic tally of the votes took place, did they match? If no, please explain what happened and how polling officials explained the discrepancy.

_____
_____
_____

## Postelection Custody and Security

| | Direct Observation | | Reported to Our Observers | | Not Observed or Not Applicable | |
|---|---|---|---|---|---|---|
| 29. Are all removable memory devices removed from the equipment? | Yes | No | Yes | No | N/O | N/A |
| 30. Is there a clear and documented chain of custody for the equipment and the saved data?* | Yes | No | Yes | No | N/O | N/A |
| 31. Is all equipment appropriately secured in preparation for storage until the next election?* | Yes | No | Yes | No | N/O | N/A |

Comments

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

# The Carter Center at a Glance

**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.

Martin Frank

THE
CARTER CENTER


The Carter Center

One Copenhill
453 Freedom Parkway
Atlanta, GA 30307
(404) 420-5100 ◆ Fax (404) 420-5145

www.cartercenter.org