THE
CARTER CENTER

2010

Waging Peace. Fighting Disease. Building Hope.

sufficient time to correct any identified errors.

During its limited observation, The Carter Center observed the automated election system (AES) in use. Under an AES, appropriate technology for voting and electronic devices is used to count votes and consolidate results. The Carter Center noted that use of electoral technology generally proceeded smoothly on election day; however, insufficient protections existed to ensure voter privacb8 Acorrect forexisted correci 8ated4.46 0.ria,ee0-7.776 c;n5dsted th0ceb8-25(teotevisns)]T6 0

C C P

With the permission of the Philippine Commission on Elections, The Carter Center deployed a limited technical observation mission to the May 2010 elections in the Philippines that focused on the use of automated

The Carter Center assesses electoral processes on the basis of an observed country's domestic legislation, political commitments relating to the electoral process, and international human rights obligations. The Philippines, through a process of ratification, has committed itself to uphold a number of international human rights treaties relevant to the conduct of genuine elections (see Figure 1). These treaties guarantee such basic rights as universal and equal suffrage; secrecy of the ballot; freedom of assembly, association, and movement; equal treatment for all people before law; and the right to an effective remedy for the violation of protected rights. The Constitution of the Philippines includes many such rights, notably through Articles III, V, and XIII.[2] Given its limited scope, the Carter Center's mission did not systematically evaluate the extent to which the electoral process as a whole upheld all such rights; however, the Center's assessment of the electoral technology adopted by the Philippines includes consideration of the impacts this technology may have on fundamental rights protected by the Philippine Constitution and public international law.

In the 2010 election cycle, the national offices at stake included the presidential and vice presidential offices, 12 of the 24 seats in the national Senate,[3] and all seats in the House of Representatives. In addition to national executive and legislative offices, a number of local races were also contested in the May 2010 elections. These included provincial governors and vice governors, municipal mayors and vice mayors, and provincial and municipal legislatures and coun-

cils. In total, between national and local offices, voters chose candidates for over 20 elective seats in May. Elections for barangay-level (neighborhood) offices were not held on May 10, 2010, but instead occurred on Oct. 25, 2010.

Multiple laws govern the

provides COMELEC with a mandate to include the identification and provision of such a system as it deems suitable and defines requirements for minimum system capabilities, procurement policies, external evaluation, testing, canvassing of election returns, and results audits.

Republic Act 9369 generally provides a broad overall basis for the successful adoption of an electronic voting system, focusing on issues such as efficiency,

A

Historically, elections in the Philippines have been marked by concerns about corruption, insecurity, and a lack of transparency. Low public confidence in elections was abetted in part by slow consolidation of vote returns and the announce-

B

An independent and impartial electoral authority that functions transparently and professionally is internationally recognized as an effective means of ensuring that citizens are able to participate in a genuinely democratic election and that other international obligations related to the electoral process can be met.[22]

Elections in the Philippines are organized by the Commission on Elections (COMELEC). The role and mandate of COMELEC are defined by Article IX of the Constitution of the Philippines as well as by Article VII of the 1985 election law. The constitution requires that COMELEC comprise seven members, including one chairman and six commissioners (the majority of whom must have passed the Philippines bar), appointed by the president to a nonrenewable seven-year term.[23] Legally, COMELEC enjoys independence, although it is subject to limited oversight by organs of the judicial and legislative branches. COMELEC's procedural rule-making powers, as provided by Section C2.1 of the Constitution of the Philippines,[24] are overseen directly by the Philippine Supreme Court, while its organizational actions and personnel are subject to investigation and subpoena by the Congress, which can order special investigations and hold hearings on electoral matters.

COMELEC's powers are wide-ranging, including the enforcement of all "laws and regulations relative to elections" and jurisdiction over all election disputes for subnational offices.[25] Article 52(i) of the 1985 election law confers responsibility on COMELEC to adopt electoral technologies as it sees fit. Under this act, COMELEC has a broad mandate to identify an appropriate system, determine voting

COMELEC's powers are wide-ranging, including the enforcement of all "laws and regulations relative to elections."

and counting procedures and locations, conduct voter education, oversee material procurement (including technology, ballots, and ballot boxes), and conduct a public source code review.[26]

Section C2.4 of Article IX of the constitution further provides COMELEC the wide-ranging power to "deputize … law enforcement agencies and instrumentalities of the Government, including the Armed Forces … for the exclusive purpose of ensuring free, orderly, honest, peaceful, and credible elections." The constitution also gives COMELEC the power to regulate all government-owned franchises, permits, or grants (such as those provided to media outlets or public transportation) during the election period as necessary[27] and to enlist impartial, nonpartisan groups in order to assist in the implementation of the law as appropriate.[28] This mandate effectively allows COMELEC to dispatch, with legislative approval, the Philippine National Police and armed forces of the

---

22 United Nations Human Rights Committee, General Comment 25, paragraph 20.

23 Constitution of the Philippines, Article IX, Section C1.1; this article further provides that commissi25(Uniteulan025(Ele-25(1985)-25(election)umd219 40229
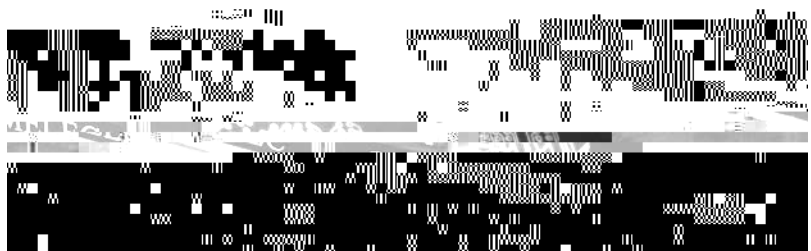
Philippines for the promotion of security and political stability during the period immediately preceding election day and to engage the services of any government agency as deemed appropriate throughout the electoral period.[29] In the 2010 elections, COMELEC utilized this power to engage the assistance of information-technology-literate members of the civil service in implementing the optical mark recognition (OMR) voting system and to request the assistance of the Philippine armed forces in distributing voting materials to remote and insecure locations.

A   B   C   C

The introduction of new technology into the electoral process necessarily impacts the structure for administering the elections and requires a higher degree of technical knowledge among election commission staff. In this light, Republic Act 9369 called for the establishment of various governmental bodies to provide advice and technical assistance to COMELEC throughout the process. In 2010, in addition to creating a Project Management Office to oversee the implementation and operation of the OMR system, COMELEC established the following advisory bodies to aid and assist its efforts:

The Technical Evaluation Committee. The committee was made up of key leaders from government, industry, and civil society. The committee was legally tasked with obtaining the certification of the automated election system (AES) by an established, international certification entity and thereby determining whether the AES, including its hardware and software components, was "operating properly, securely, and accurately." In addition, the committee was required to ensure the proper review and retention of the source code by a secure third party (The Central Bank of the Philippines).

Posters in COMELEC's media center provide basic information on the elections and the new technology.

The COMELEC Advisory Council. The council is made up of nine members from national departments, academia, the information and communications technology field, and nongovernmental electoral reform organizations. During the 2010 elections, the council was tasked with recommending the most appropriate, secure, and cost-effective technology and with participating as nonvoting members on the Bids and Awards Committee. While the council had no official duties related to the implementation of electronic voting technologies, it was ultimately responsible for the following:

- RECOMMENDING VOTING SYSTEMS
- PLANNING AND TESTING SYSTEMS
- IDENTIFYING ISSUES
- DESIGNING PLANS FOR THE BID PROCESS, use, and eventual disposal of AES
- CONDUCTING EVALUATION OF PHASES

---

29 The 1985 election law, Article 52(b) limits the ability of COMELEC to deputize government instrumentalities and military forces to the campaign period and "thirty days thereafter."
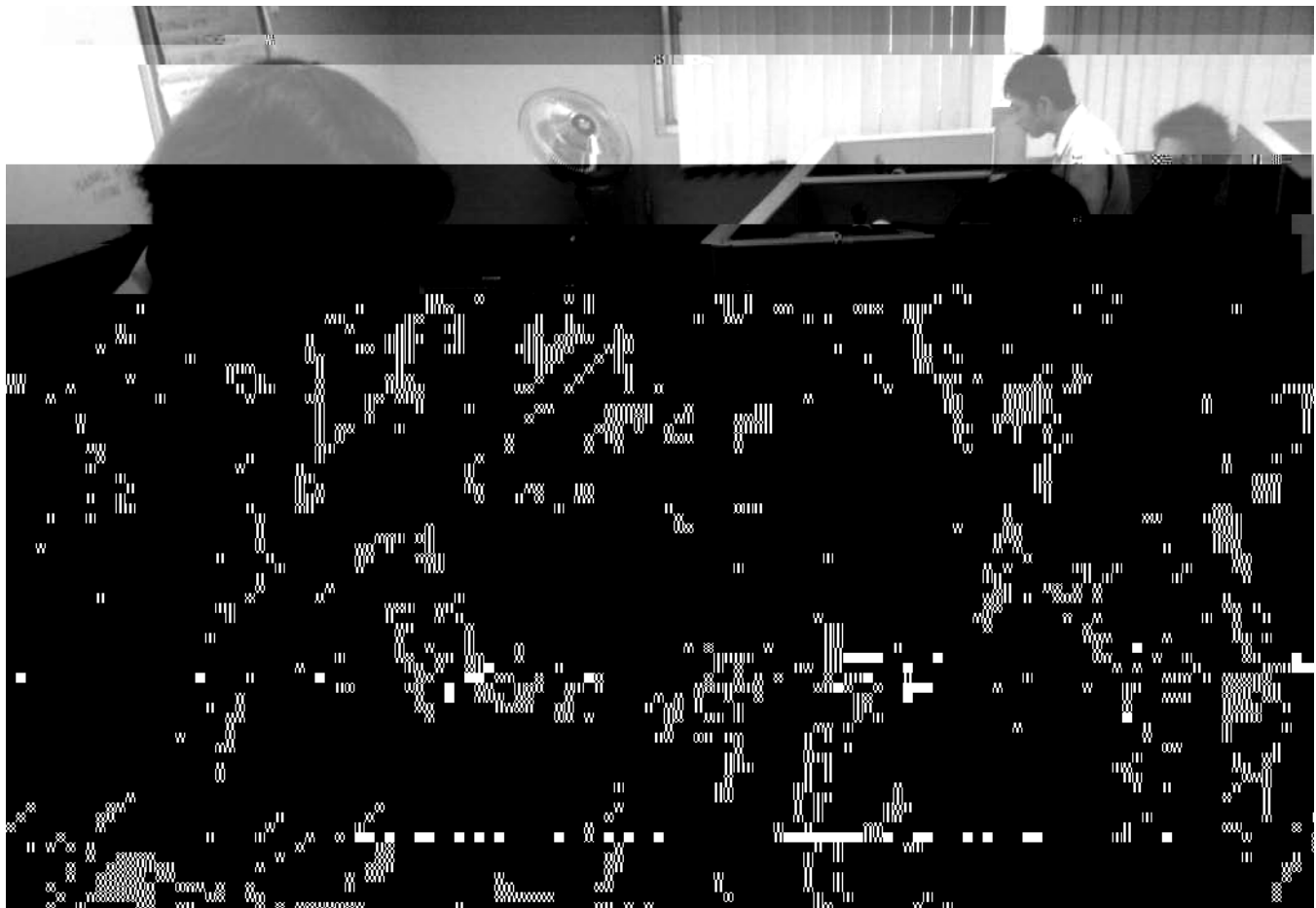
A Smartmatic technician instructs the Board of Election Inspectors (BEI) officials on the function and proper working of the PCOS machine for election day operation.

operation of the AES. According to the contract, "The entire processes of voting, counting, transmission, consolidation, and canvassing of votes shall be conducted by COMELEC's personnel and officials, and their performance, completion, and final results according to specifications and within the specified periods shall be the shared responsibility of COMELEC and the provider." In practice, COMELEC retained the responsibility for hiring electoral workers, for selecting precinct and canvassing center locations, and for coordinating security in areas known for violence or political unrest; however, most technical and logistical duties were eventually completed by Smartmatic and other technical service provider corporations, with COMELEC providing oversight.[33] While the unfamiliarity of the

AES required significant input and oversight from Smartmatic in 2010, in future elections COMELEC, as the legally mandated election management body of the Philippines, should seek to increase its capacity to oversee the technical aspects of the process. Smartmatic officials often conducted press interviews and voter education efforts, responsibilities more clearly mandated as COMELEC's, and which may be better completed by the commission itself in future elections.

---

33 Subsequent and separate contracts with Smartmatic included a 519-million-peso contract for the procurement of ballot boxes and transportation of PCOS machines to all polling centers nationwide as well as another contract for 499 million pesos to cover delivery services for the ballots.
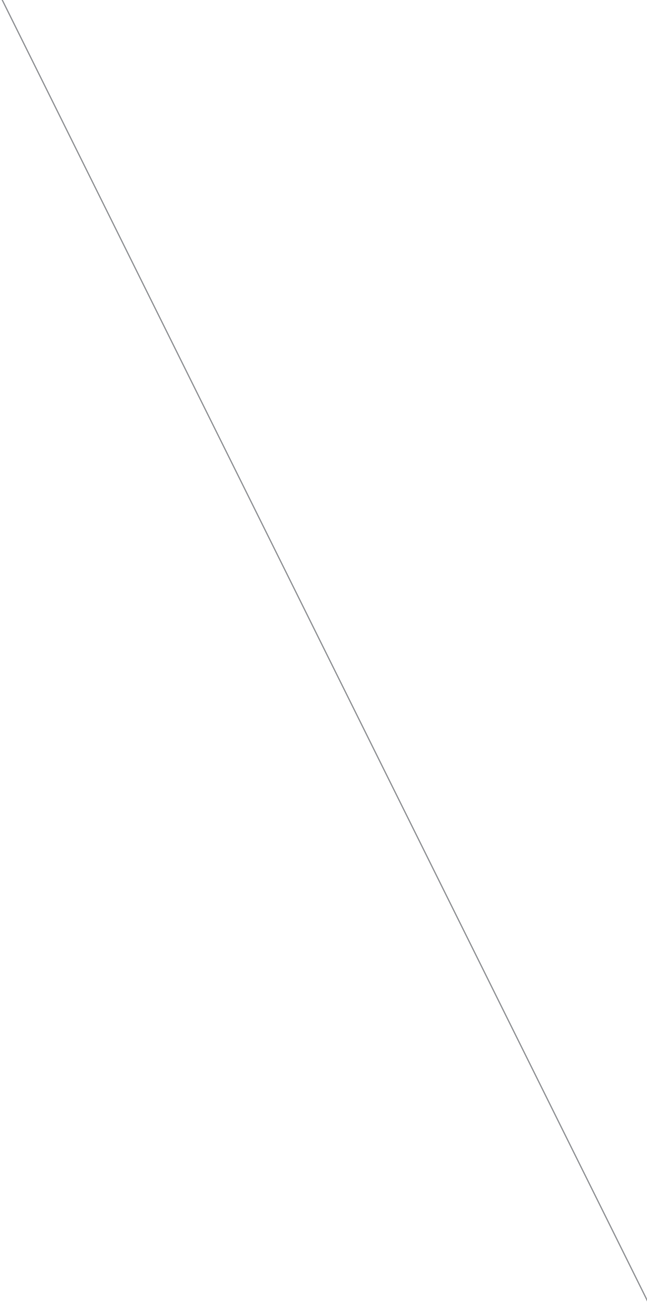
backup card was to be placed in the administrator slot
and sealed by the BEI only after testing and sealing
took place.

## Results Transmission and Digital Signatures

In the initial request for proposals for the automated
election5(the)8Fsm-0.783 -0.7 l-M25(LimiOMELEC783 -0.tan)-25(to-25(to)--25(automated)]TJ0 -.5Cpos.-9-28OpP)-25.

Trusted Build and Hash-Value Verification

A "trusted build"—the process of turning the original source code into machine-executable code—occurred on Feb. 4, 2010.[42] While no official record was provided as to who witnessed the trusted build, COMELEC reported to Carter Center observers that the process remained open to party officials, candidates, and their representatives. The hash values, or indices that match data sets in an array (such as filled-in oval marks to indicate candidate names) were published in a COMELEC resolution and posted on the website. According to COMELEC and Technical Evaluation Committee (TEC) officials, the configuration of the machines—including the loading of firmware and hash checking—was conducted from February to mid-April; however, exact dates were not provided.[43]

Carter Center observers were unable to obtain any documentation on the procedures for or results of these verification activities. In addition, The Carter Center was informed by COMELEC that the Philippine political parties and the Parish Pastoral Council for Responsible Voting, which served as the citizens arm in this election, were provided with the firmware's digital signature, which could then be verified against that listed on the initialization report printed by the PCOS on election day; however, it was unclear to Carter Center observers whether such verification took place.

C C
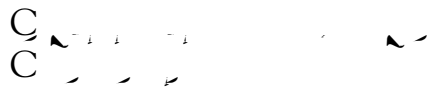
Critical to the implementation of any automated voting technology are the thorough and transparent testing, review, and certification of all system components prior to use.[44] Bound by Resolution 9369, COMELEC, via its Technical Evaluation Committee, is required to certify that "the AES, including its hardware and software components, is operating properly, securely, and accurately." The resolution provides that such certification must include documented, successful reviews of the following procedures: (1) field tests and mock elections; (2) an audit of the

accuracy, functionality, and security controls of the AES software; (3) a source code review; (4) storage of the source code at the Philippines Central Bank; (5) confirmation that the source code review was conducted on the actual source code installed on election equipment; and (6) development of contingency plans for each component and sequence within the AES system. The committee issued its final certification, affirming that the above requirements had been properly, securely, and accurately met in a resolution dated March 9, 2010.[45]

SysTest Labs, an American software and source code testing and auditing firm, carried out steps two and three of the certification. SysTest's review covered almost all of the software, hardware, and transmission components involved in the election.[46] Election system software was reviewed against both Philippine election law as well as specific certification criteria of the Voluntary Voting System Guidelines published by the U.S. Election Assistance Commission.[47] On the critical issue of whether the AES software tallies votes accurately, SysTest stated in its final report that the firm's "manual and automated review of Smartmatic's election management system and consolidation/canvassing system source code, as well as Dominion's election event designer and precinct count optical scanner source code, revealed no evidence of any intentionally written instructions to yield any but the correct results."

---

42 Carter Center observers had not yet arrived in the Philippines.

43 Interview with COMELEC and TEC, June 10, 2010.

44 It is recognized good practice that the state should ensure the reliability and security of the e-voting system and that an independent body be charged with this task (Recommendation of the Committee of Ministers of the Council of Europe, Articles 25 and 28).

45 Republic Act 9369, Section 11.

46 Excluded from the review were the ballot generation software and the architecture of the government website used to announce election results. Nor did SysTest review some aspects of the software, including the modem transmission module.

47 Available at http://www.eac.gov/vvsg.

dated in the mock election are designed and intended "to test and determine the functional capabilities and systems reliability in actual conditions and environment as on election day…in recording and reading the votes, printing of election returns, electronic transmission of results from polling places to the municipal, city, provincial, national canvassing and consolidation centers."

In actual practice as observed, mock elections were limited in all but one case to not more than 100 vot-ers and did not include manual audits to check the accuracy of the results. Critically, the design and layout of the mock election ballots did not precisely correspond with those used on election day, and the ballots used in the mock election were never compared with the results produced by the PCOS. In the future, COMELEC should consider conducting mock elections that more accurately reflect election day conditions in order to ensure the identification of potential problems with adequate time for their resolution.

D

Just as with manual, paper-ballot-based elections, ensuring a secure physical chain of custody of voting equipment (including ballot boxes, ballots, and precinct voting paraphernalia) is vital to the avoidance of any risk of fraudulent or malicious behavior. In the case of automated elections, the need to ensure strict control of the voting machines, modems, memory cards, and other electronic devices used in voting and results transmission can be even more critical, given the increased potential for unseen malfeasance and variable public trust. As such, materials should remain secure at all times, and documentation of access to the materials must be recorded throughout the election cycle—from manufacture to machine decommissioning.

B   D

Ballots were printed at the National Printing Office (NPO) under the supervision of Smartmatic and COMELEC officials. In visits to the NPO in the weeks prior to the election, Carter Center observers noted that well-organized security precautions were taken.

Prior to the ballot distribution contract being awarded, however, the finished ballots were stored in the NPO building itself, overflowing into a fenced-off area of the otherwise open main lobby of the building. While this did not necessarily represent a security threat, it represented the practical impact that the late issuance of election-logistics subcontracts had on the process and emphasized the importance of future efforts to ensure that the electoral calendar allows for proper implementation of the electoral technology to be used.

To prevent extra ballots from being produced, all electronic files used in their creation were deleted from the NPO systems, and all printing machines were sealed after the last ballot was printed. Once printed, ballots were shipped to their locations in

tamper-evident boxes. COMELEC also instituted chain-of-custody procedures that included the Philippine police or armed forces accompanying the ballot shipments to the municipal treasurers' offices as well as to their ultimate precinct destination on election day. COMELEC also maintained a warehouse in Cabuyao, Laguna, where PCOS machines were stored and configuration took place under constant security.

Access to observe the process was available to political parties and accredited observer groups. While Carter Center observers were invited on a scheduled tour of the facility on April 20, on a subsequent unannounced visit a week later, they were denied entry and were informed that prior security clearance was required to enter the facility and that they must be accompanied by senior Smartmatic staff. A second, scheduled tour along with the Parish Pastoral Council on Responsible Voting (PPCRV) and members of the media took place on May 5 to observe the reconfiguration of the system's PCOS machines. Accredited international and domestic observers should be granted access to all aspects of the electoral process.[51]

C   D

COMELEC implemented various measures to restrict unauthorized access and prevent tampering with the AES components during distribution. COMELEC informed The Carter Center that comprehensive chain-of-custody procedures had been established and that shipment of the machines from the central warehouse to the various distribution hubs around the country had begun by mid-April. The delivery plans and schedule were to be known only by COMELEC, Smartmatic, and the PPCRV—political parties reported that they were not informed of the schedule. Once at the distribution hubs, machines were

---

51 Declaration of Principles for International Election Observation, Articles 12(b) and (c).

week's time, the chosen solution consisted of altering the configuration of the primary CF cards to enable them to correctly read the misspaced ballots.[52]

All primary CF cards that had already been distributed were recalled to the configuration facility in Laguna. By using 18,000 spare CF cards that were already on hand at the configuration facility, purchasing 30,000 new cards in Hong Kong and Taiwan, and reconfiguring thousands of cards recalled from the provinces, Smartmatic managed to distribute a sufficient number of properly configured CF cards nationwide within the week. Testing and sealing were then conducted a second time in the few polling stations that had initially conducted the procedure on the first day allowed, May 3. In the great majority of polling stations, the time frame for testing and sealing was extended, with most procedures occurring on May 8 and 9. In the few areas that received the new CF cards at a later date, testing and sealing took place on the morning of the election, before polls opened.

Given the centrality of the CF cards to the functioning of the AES, the need to recall all 76,000 cards and deploy new ones within a week of election day alarmed the public and led to demands for the election to be postponed. In spite of the tight time line, however, CF cards were recalled, reconfigured, and redeployed in time for nearly all precincts to open as scheduled. Despite this, the episode raised serious questions about COMELEC and Smartmatic's testing procedures and contingency plans. The rushed introduction of new CF cards and the replacement of old

In some polling places, poll worrkers had to complete testing and sealing on the day before the election because of a compact flash card error.

ones also significantly undermined existing chain-of-custody procedures.

Furthermore, it was apparent on election day that some PCOS machines were missing seals on the CF card slots. While it is hard to pinpoint why the proper seals were not used, it seems likely that the card replacement process was a contributing, if not the primary, factor for this oversight. The Carter Center received no reports of unreconfigured CF cards being used on election day nor reports of incidents of CF cards being removed during voting because of the lack of seals; however, the confusion created by the CF card episode raised concerns about the creation and successful adherence to chain-of-custody security precautions and realistic testing schedules for future elections.

---

52 The blank backup CF cards were not affected by this reconfiguration.

they seemed otherwise comfortable with handling and
completing the ballots.

Voter education efforts at the polling station,
including having poll workers stationed by the PCOS
machine to guide voters through the process and
confirm that their ballot had been accepted and
deposited into the ballot box appeared successful
at allaying concerns about the system; however, in
some polling stations where workers (statiocB(otherwise)]TJT*[engaged,g)-25(poll)-25(atchkers)-25fromt the ir
poiticall seappd, in to guiaonco
the PCOS machine to voter.e

ay, idiucation that sugh
ay, vo
the poll atchkers
larified,g and sugh
vouidd,g aly, tirs stgco
the process whne ballot se

feeding the ballot into the PCOS machine. In many cases, voters abandoned the secrecy folder entirely and inserted the ballot directly into the

A

Electoral security must take into consideration the process by which results are transmitted to aggregation centers. In the case of elections employing automated technology, results transmission generally occurs through transmission of a digital file, making the process largely unob-servable. Given the inherent lack of transparency in secure digital transmission, observation of such processes is at best limited in nature, focusing on the legal and technical framework for transmis-sion. Under the Philippine elec-tion law, the process for digital aggregation of results mirrored the manu3e73 TD[(of)-25(trgtem)]TJ(-ugh).017 iv 575.34ious elections, with elec-tion returns transported to the board of canvassers, Parish Pastoral Council on Responsible Voting (PPCRV) and COMELEC; however,(-ugh)of ad of physical returns being 5.3pared and delivered, digital results are

ment. The precinct that was ready to transmit results first would use the transmission equipment and then pass it along to the next station when its transmission was completed. From the polling stations, results were transmitted sequentially and separately to servers at the Municipal Board of Canvassers, KBP/PPCRV in Manila, and the COMELEC backup server in Manila.

If transmission was not successful after three attempts, a Smartmatic technician would be called to the precinct to provide technical support. After successful transmission, an additional 22 copies of the election returns were printed and distributed to various parties,a Soties,a h5(server)ervm396 1.0,a 6 1iv diide 8 to s25(be)-25(called)]TJ0 -cinct From the polling precinct l

results soon after they were received at the central server on a government-hosted, publicly accessible website, and poll watchers throughout the country were able to confirm their precinct-level printed returns with the figures published at the national level.

C   C

Complications occurred during the canvassing process. Results from each clustered precinct were to be aggregated at the Municipal Board of Canvassers (MBOC), where the winners for local races are declared. The MBOC also sends the aggregated results for offices at the provincial and national level to the Provincial Board of Canvassers (PBOC). The PBOC aggregates all the results from its constituent MBOCs and declares the winners for provincial offices. The PBOC then transmits the aggregated results for offices at the national level to the National Board of Canvassers (NBOC). The NBOC is responsible for aggregating the results from all the provinces in the country as well as overseas ballots and declares the winners for national offices.

The original COMELEC rules, and hence the configuration of the canvassing software, specified that canvassing centers could only proclaim winners and transmit results up the chain after receiving returns from 100 percent of its constituent stations or boards of canvassers. As it became clear that there would be a few polling stations in many districts with transmission difficulties, however, COMELEC issued a resolution that lowered the thresholds for transmission and proclamation. If the number of outstanding votes would not be enough to affect the standings of contestants in a specific race, canvassing centers were authorized to proceed with proclamations for races at their jurisdictional level. Although the resolution did not specify the threshold that must be reached prior to the proclamation and transmission of higher-level results, in practice, it fell in the 93 to 95 percent range.

Random Manual Audits

According to Republic Act 9369, a random manual audit (RMA) was to be conducted in at least one clustered precinct in each of the country's 229 legislative districts on election night. In the face of criticism by some groups about the small size of the sample, COMELEC adopted Resolution 8837, dated April 30, which required that five clustered precincts be audited per district, resulting in an audited total of 1,145, or 1.5 percent of the total number of PCOS used on election day.[63] Three hundred and fifty barangays (neighborhoods) were excluded from the RMA selection pool because they are too difficult to reach.

The RMA was known as a "cold audit," as it had no impact on the election proclamation but rather was merely a step to verify the accuracy of the electronic counting by the PCOS machines. RMAs were to be conducted according to the following procedure: immediately after the tabulation and electronic transmission of results were complete, the random manual audit team (RMA team) would enter the selected precinct and take custody of the sealed ballot box.[64] If the number of ballots counted exceeds the number of votes recorded to have been cast, the RMA team would randomly select a number equivalent to the excess and remove them prior to counting. Witnessed by party representatives, the RMA team would count votes for president, vice president, Congress, governor, and mayor and record the totals on a large tally board posted on the wall of the precinct. After completing the audit, RMA teams would determine the reason for any variance between the AES and RMA results and record this on the audit return, which would then be transported to the provincial election supervisor and subsequently to COMELEC for analysis by the National Statistics Office and the random manual audit technical working group.

The random selection of precincts was to be conducted at noon on election day at the operations center for COMELEC and led by the RMA technical working group.[65] Selection was to occur through the drawing of five numbered balls for each district, corresponding to precinct numbers to be audited. Carter

A COMELEC official conducts the postelection random manual audit of tally votes received for candidates.

Center observers were not present at the drawing but did receive reports that this process was not followed, resulting in a significant lack of transparency. COMELEC reported to Carter Center observers that confusion around the order of selection of the precincts led to a delay in drawing the balls, and with limited exceptions, no information was distributed or posted publicly as to which locations were to be audited. As no official minutes of the RMA selection were kept, it was also unclear who was present at the drawing.

In addition, there was a delay in informing the RMA teams of their assignments until after polls had closed and the ballot boxes had been taken to the

---

63 It is good practice, when performing postelection audits, to select machines from each local jurisdiction, given that each will have a different configuration based on local races.

64 It is important to note that the RMA team had not served as BEIs during election day so that they would be able to conduct the RMA without being fatigued.

65 The selection of random precincts on election day itself, rather than prior to it, is an effective policy, as it reduces the risk of targeted fraud based on a predetermined list of precincts to be audited.

municipal treasurer's office for storage. To remedy these difficulties, COMELEC passed a resolution allowing for the audits to take place at the treasurer's office rather than in the precinct. In many cases, when the RMA teams arrived at the municipal treasurer's office to conduct the RMA, the treasurers were reluctant to allow them access to the ballots, as they had not been informed of any changes in procedure. COMELEC cited a malfunctioning fax machine as the reason for the delay in notifying the treasurers of the RMA teams' assignments. This compounded the initial delays in communication and caused significant delays in the conduct of the RMA as a whole.

Despite delays, once completed, the RMA did not show significant discrepancies in results. As reported on May 29 by the Parish Pastoral Council on Responsible Voting (PPCRV), which was responsible for reporting on the RMA to COMELEC, with 1,063 audits completed, "minimal variance" had been deter-

mined. There was 100 percent accuracy in 80 percent of RMA tallies on a candidate-by-candidate basis, while 6 percent of precincts recorded single-digit variances, and 14 clustered precincts reported double-digit variances.[66] The largest discrepancy reported between digital and manual results was 99: 352 on the printed election report as compared with 253 on the audit report. Because of the similarity in numbers, however, it seems likely that this was due to a transcription error made by the BEI.[67]

According to COMELEC, discrepancies were generally attributable to errors in manual transcription by the RMA team when recording the totals to the AES and RMA tallies. In the event that unexplained discrepancies existed after this process, a root cause analysis took place—the PCOS and compact flash cards of the clustered precinct in question were retrieved and examined, including hash code and configuration audits. Carter Center observers were informed that one errant PCOS machine, which had registered a large number of overvotes for one local race, was determined to have an ink mark on the scanner inside the machine. Observers were shown a picture of the scanner in question; however, it was unclear to COMELEC officials how this mark was made on the scanner or whether the discovery would lead to an expanded audit of the PCOS machines.

PPCRV volunteers compare hard-copy results from polling stations with results on the online server.

66 Because results of the RMA were not made public, The Carter Center has relied on interviews with civil society groups and election officials for accounts of the RMA's accuracy.

67 Carter Center observers requested to enter the RMA verification room at COMELEC where manual RMA forms were being verified against the election returns printed by the AES on three occasions. On two of these occasions, observers were denied access by COMELEC for "security reasons." On the one occasion when observers were granted access, they noted that most audit returns they were able to view had only minor discrepancies between the AES and RMA tally, which were generally fewer than five votes. However, they observed one precinct audit form that contained an unusually high number of differences in votes for mayor and governor, with variances of up to 94 votes. No explanation was recorded for this variance. Carter Center observers were informed by COMELEC officials that in the event of discrepancies, a thorough examination of the returns and paper ballots would be conducted by COMELEC staff in Manila; however, The Carter Center was unable to determine whether or how this process took place.

As of May 18, PPCRV had received 70,255 of the 76,347 returns (92 percent nationwide) and had entered approximately 50,000 of them. Of the encoded election returns, 29 discrepancies had been discovered, which reflected four types of discrepancies, as illustrated below in Figure 3. COMELEC officials explained to Carter Center observers that the types of discrepancies covered in #3 and #4 of Figure 3 have occurred when BEIs did not follow the correct procedures and transmitted testing and sealing results that were contained on the backup compact flash card. No explanation was offered to The Carter Center for the #1 and #2 discrepancies.

Figure 3. Four Types of Discrepancies in Vote Returns

Discrepancy Type	Fourth Election Return of PPCRV, Manually Encoded	Transmitted Data in Server (Pius)	Number of Incidences to Total Election Returns Entered
1	Reflects votes cast	Transmitted zero votes	4 precincts (0.01 percent)
2	Reflects votes cast	Transmitted all votes cast with exception of one candidate wherein transmitted result was lower by one count	2 precincts (0.005 percent)
3	Reflects votes cast	Transmitted votes with numerical values of less than 10	19 precincts (0.05 percent)
4	Reflects votes with numerical values of less than 10	Transmitted votes cast	4 precincts (0.01 percent)

Source: PPCRV

such keys was completed by the technology vendor, Smartmatic, rather than an external body, potentially leading to questions about the transparency of the process. Furthermore, review of the AES's source code was limited to an on-screen presentation conducted under the auspices of COMELEC. Concerned that such a review was inadequate to identify potential problems, many watchdog groups chose to forgo participation and were unable to review the code at all. In the future, consideration should be given to increasing access to the source code while maintaining necessary security. Whether the source code is ultimately made fully public or not, legal regulations should be made more specific as to the conditions under which source code review is permitted by non-contracted parties outside the official certification and software audit.

The Carter Center notes positively COMELEC's commitment to make available pertinent electoral information on its website, including the electoral calendar, all COMELEC resolutions, and portions of its vendor contracts; however, in order to promote even greater transparency in the procurement and contracting process, The Carter Center recommends that all pertinent documentation regarding vendor and commission relationships be made publicly available.

6. Amend procedures to ensure secrecy of the ballot, in law and in practice.

The Carter Center observed significant curtailment of the right to vote by secret ballot in the 2010 elections. While this lack of secrecy did not appear to lead to voter intimidation or to undermine the credibility of the process, it does represent a departure from recognized international law and should be rectified in future elections. Amendments to the election law removing the requirement for a provision of voting booths may be reconsidered. In addition, while ballot secrecy folders were provided in each polling station, in practice these proved ineffective and were often abandoned altogether. This, coupled with the common practice of BEI staff's checking of ballots initially

rejected from the PCOS machine for stray marks, effectively undermined secrecy. Future electoral processes will benefit from increased measures to ensure privacy during voting and increased secrecy measures during the casting of ballots.

7. Ensure measures to increase security meet their ends while upholding fundamental rights and ensuring cost-effective electoral processes.

COMELEC took significant measures to provide for ballot security in the 2010 election. COMELEC ordered the creation of only the exact number of ballots necessary for registered voters and ensured the printers and ballot design files were incapacitated after printing was complete. In addition, each ballot was to contain an ultraviolet mark of authenticity. The intent of such measures was commendable, attempting to address a legacy of electoral fraud.

In practice, however, these measures were not always effective. For example, when the PCOS scanners could not read and authenticate ultraviolet markings on the ballot, COMELEC procured and distributed handheld UV lamps for ballot authentication. These lamps were not widely used. The utility of such security measures, in light of other authentication measures, such as the timing codes present on all ballots, should be reviewed in light of efficiency and economic concerns.

More significantly, the decision not to provide additional ballots that could be used in the case of ballot spoilage has the potential to severely impact the universality of suffrage by unfairly disenfranchising voters. As such, the Philippines should reconsider these restrictive provisions in the law, potentially returning to past provisions that allowed a set percentage of additional ballots to be distributed to each polling station.

8. Consider expanding the number of polling stations and dividing larger clustered precincts in order to minimize delays in the voting process.

As a cost-saving measure to reduce the number of PCOS machines required, COMELEC decreased

A

B
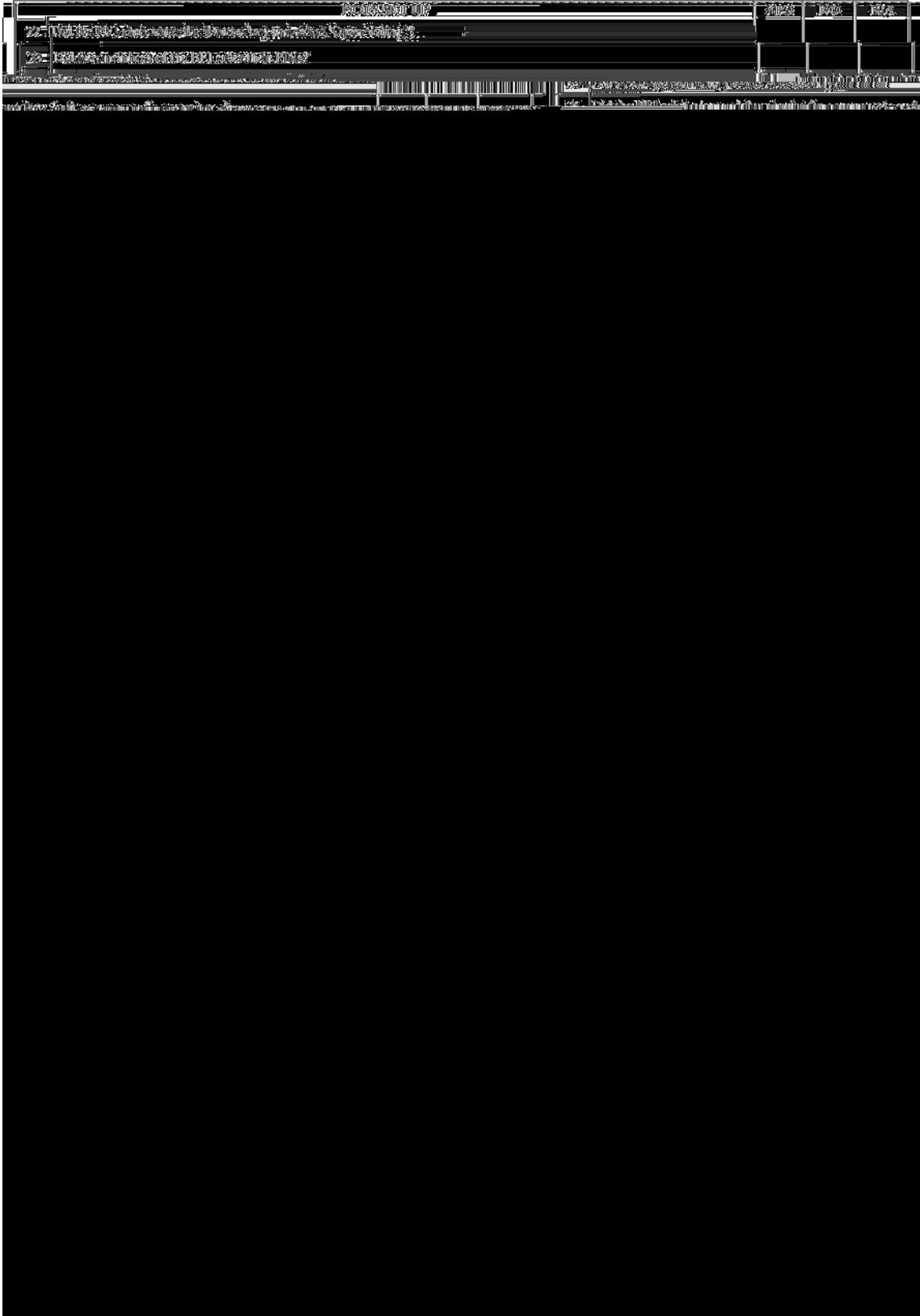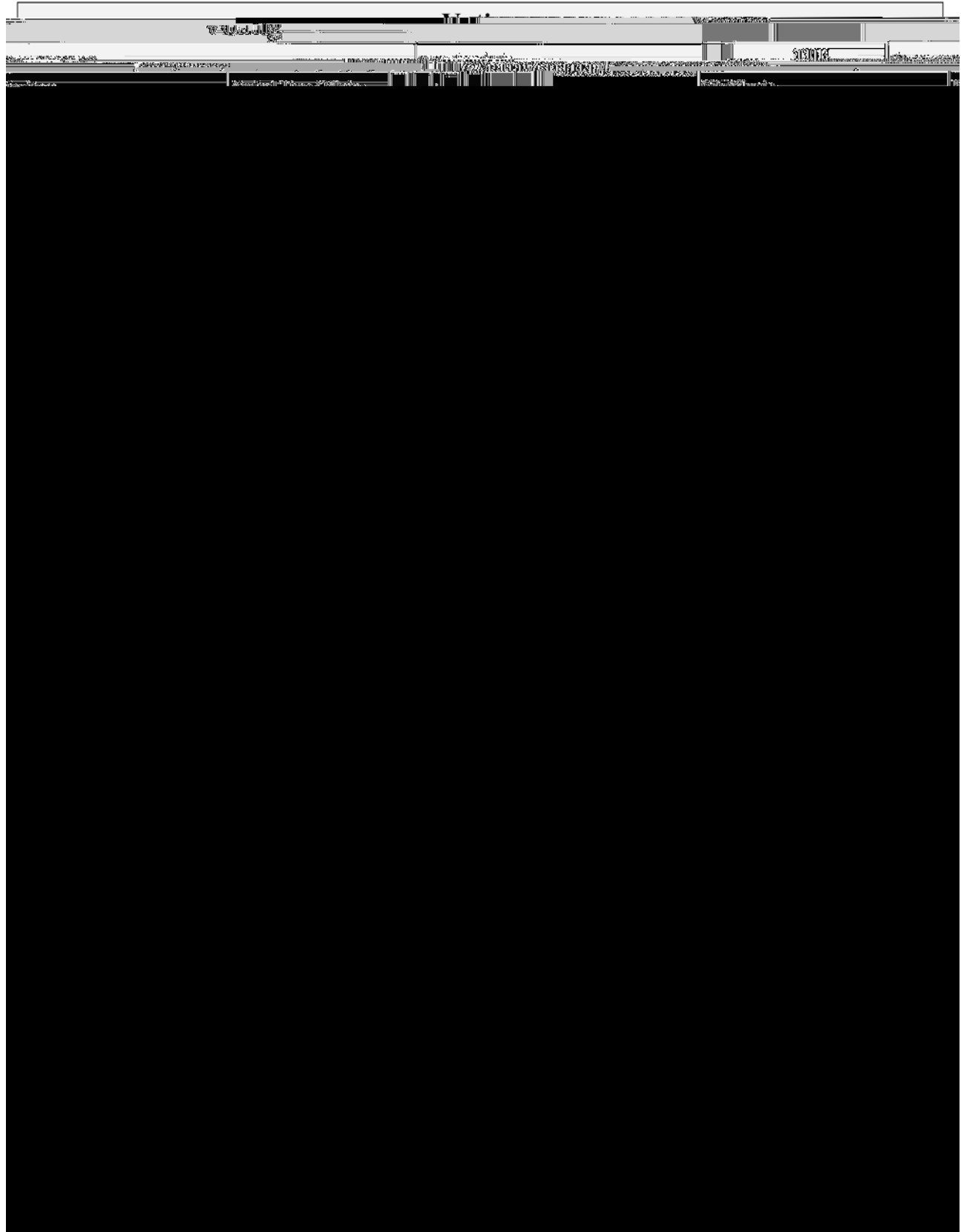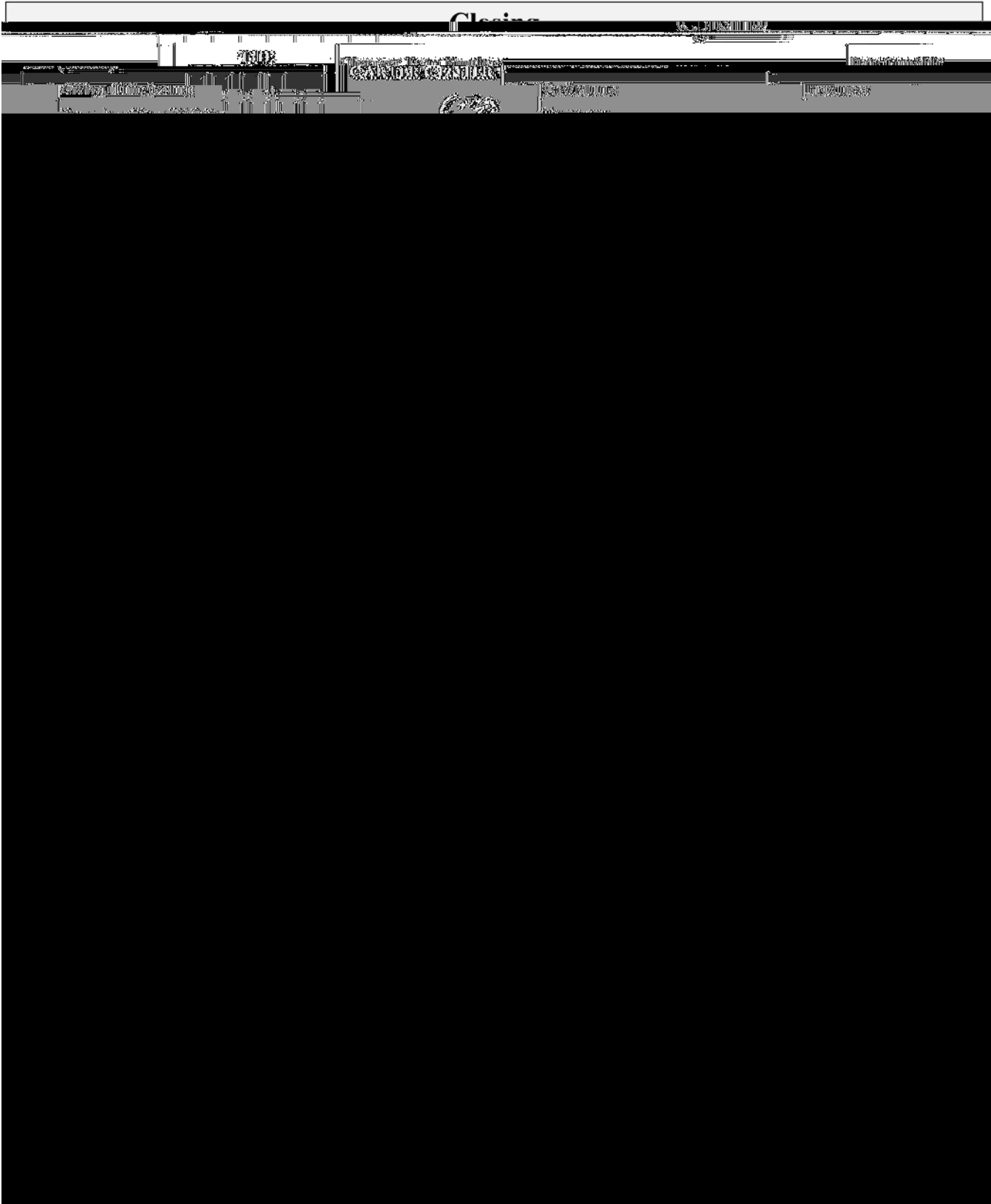
Instructions for Completion

This baseline survey has been developed with the intent to help observers collect and process all relevant data associated with electronic voting technologies. The information gathered by answering these questions should create a comprehensive picture of the voting system in use and thus allow a fuller 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, technological standards against which the technology is measured, reports on past processes, etc. Please be sure to include details on how, where, and when the information was attained and, particularly in the case of interviews, the name, title, and affiliation of the source of the data. It is anticipated that this process will occur over a number of weeks in the months leading up 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 (long-, medium-, and short-term) as a point of reference for their observations. In addition, data collected will be used to formulate and modify more generic election day (and other) checklists to capture information on the actual functioning of the system.

survey. Many questions asked under the legal framework section are inextricably linked to other sections of the survey. However, for ease of use, all questions relevant to a review of the election law have been grouped together. Therefore, legal framework questions (excluding those dealing with the complaints and disputes procedures, which do not appear elsewhere in the survey) are tagged with a second acronym identifying them to their relevant section of the survey. These acronyms are based on the subheadings which appear in the baseline survey and are as follows:

‡ Technology and System in Use: TS
‡ Public Confidence in the Technology: PC
‡ Accessibility: A
‡ Institutional Organizations: IO
‡ Technology Vendors and Procurement of
  Equipment: VP
‡ Certification and Testing: CT
‡ Acceptance Testing: AT
‡ Other Pre-election Testing: PE
‡ Election Day Testing: ET
‡ Security and Integrity of the System: SI
‡ Software: S]TJ/C2_0 1 Tf-0.941 -1.273 Td00087Tj/Span/ActualTextFEFF0020BDC 0003TjEMC /T1_1 1 Tf/Span/ActualT
‡ Cology abulathon]TJ/C2_ 1 Tf-0.941 -1.273 Td00087Tj/Span/ActualTextFEFF0020BDC 0003TjEMC /T1_1 1 Tf/Span/Ac

describe the bidding and tendering process for e-voting technology. Is it transparent and competitive? (Please describe and attach any supporting documentation.) (EMB, V)

57) What vendor/s provide which components of the electronic voting systems? Please describe. (V, EMB)

58) Have the vendors described in question 55 made contributions to political parties or campaigns? If so, please describe and attach any relevant documentation. (PP, V, CS)

59) 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) (EMB, V)

60) Please describe the plans in place for troubleshooting during each element of the process? (V, EMB)

61) What, if any, penalty or reimbursement provisions are triggered by technical problems with the technology? (V, EMB)

Security and Integrity of the System

62) Please provide a detailed description of the technologies in place to ensure the physical security of the electronic voting system (for example, tamper-evident seals) before, during, and after election day, including who is allowed physical access to the equipment, what measures are taken to prevent physical tampering with the election equipment, whether or not physical access is documented, and who maintains those records. (EMB, V)

63) 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 (this)-25gy or rei0EMB, a election day, including wwith theJ-1.164 t after ana22 0cEles c

other uses of the equipment, including the purpose, who has physical access, other software that is required for this secondary use, etc. (V, EMB)

72) What is the method of transmission of information between the components of the system? Please describe. (V, EMB)

73) If possible, please provide a detailed description and diagram of all of the data paths in and out of the components of the system. (V)

74)

90) What contingency plans are in place in the event of failure of the central tabulating computer? Please describe. (EMB, V)

Contingency Planning

91) What contingency planning training is in place for polling officials? Please describe and attach any pertinent information. (EMB)

92) How do polling places and central offices communicate in case of emergencies, such as power outages, telecommunications failure, etc. (EMB)

93) What happens if a machine is found to have been tampered with? Please describe any contingency plans that may be in place for such an event. (EMB, V)

C

Certification and Testing

94) What is the certification process? Please describe the process in detail, including the relationships between the different certification processes, and attach any relevant documentation. (EMB, V)

95) Does certification occur before or after the procurement process? (EMB)

96) What standards are applied to the certification of e-voting technologies? Please attach relevant documentation. (EMB)

97) Who is responsible for this certification? (EMB, V)

98) Who pays for the certification of the technology? (EMB, V)

99) Is the technology recertified after every upgrade and repair? (EMB, V)

100) What is the relationship between the certification body and the organization whose technology is being certified? (EMB, V, CS)

101) Is the certification process accessible to the public, political party agents, domestic observers, or international observers? (CS, PP, EMB)

102) In Td( )TjEMC 5j/S n -2.164 -1.818 7ystemaobserversrevie

130) Are the public, party agents and observers allowed to observe the postelection audit? (EMB, CS, PP)

131) Is the public notified of the time and place of the postelection audit, and if so, how? (EMB, I, CS)

Acceptance Testing– A series of tests run on an operating system to test particular features of the system prior to launch of the product.

Audio Ballot Functionality — The working capacity of the audio verification component of automated election machine technology.

Ballot Database– The electronic database within a server that maintains records of all votes recorded.

Central Count Optical Scan (CCOS)– A voting system that tabulates ballot results from multiple precincts in one location and, depending on the technology, creates either/both a printed report or/and an electronic report.

Central Tabulating Computer– A single server that collects all precinct polling data and tabulates the results together at a national level.

Certification — Also known as product qualification, a process by which a certain product (in this case an electronic voting machine) is ascertained to have passed certain previously stipulated qualification requirements.

Certification Body— An independent and administrative authority that determines whether the voting equipment has met the set of preapproved standards through a process of certification.

Chain of Custody— Chronological documentation of the seizure, custody, and transfer of an item.

Cold Audit — An audit of electoral results completed sometime after election day, used as a way to verify that all technology was functioning correctly but generally not intending to impact the electoral results.

Direct Recording Equipment (DRE)— A voting machine system technology that records votes by means of a touch screen or keyboard-user interface.

Election Audit — A verification process, ideally through the keeping of a paper record of electronic voting data, used to authenticate results and verify the validity of the electoral contest.

Executable Code– As opposed to a file that only contains data, executable code contains instructions or commands for a computer processing unit or its software.

Firmware— The programmed instructions that compose the circuitry of an electronic device.

Functionality Test— A type of testing that determines whether or not the data entry interface correctly recognizes and records data entry inputs.

Hardware— The physical and tangible components

software.

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 nongov-
ernmental organization, the Center has helped
to improve life for people in more than 70 c(Cai5-1.22653lhfQq 1 S1 gss04 clv)Tj3a7lnflicts; and