THE FINAL STRETCH: GEARING UP FOR THE MAY 10 AUTOMATED ELECTIONS

An EU-CenPEG PROJECT 30-30 PRELIMINARY REPORT on the 2010 Automated Elections
Period covered: January 15-March 31, 2010

Published by the Center for People Empowerment in Governance (CenPEG)
through the EU-CenPEG Project 3030: Action to Protect the Integrity of the Vote and Transparency in the 2010 Elections
First Publication: October 28, 2010

THE FINAL STRETCH: GEARING UP FOR THE MAY 10 AUTOMATED ELECTIONS

An EU-CenPEG PROJECT 30-30 PRELIMINARY REPORT
on the 2010 Automated Elections
Period covered: January 15-March 31, 2010
Released: October 28, 2010

CONTENTS

PROJECT 30-30 PRELIMINARY REPORT
Period covered: January 15-March 31, 2010
EU-CenPEG Project 3030
Released: October 28, 2010

I. INTRODUCTION

The preparations for the first fully-automated national and local elections in the country have entered the critical period. With less than a month before the May 10 elections, various watchdogs and monitoring groups, including AESWatch and the Joint Congressional Oversight Committee, have been watching closely the preparations of the Commission on Elections (Comelec) and that of the winning bidder, Smartmatic-TIM. One of the groups that have been closely studying the automated election system (AES) since the Autonomous Region of Muslim Mindanao (ARMM) automated elections in 2008 is the Center for People Empowerment in Governance (CenPEG), a policy study center based in the University of the Philippines.

CenPEG has come out with four major studies related to the automated election system. The first is, CenPEG Observer's Report on the August 2008 ARMM Automated Elections. This was followed by *Comelec's PCOS-OMR* System Rejects Public Counting, Enhances Wholesale Cheating (May 7, 2009); the *30 Vulnerabilities and 30 Safeguards* document (October 2009); and The Automated Election System 2010 of Comelec: Challenges and Uncertainties: A Preliminary Study of the AES (May – August, 2009) in partnetship with the Office of Dean Marvic MVF Leonen, College of Law, University of the Philippines (October 27, 2009).

Among others, CenPEG's research revealed that there are 30 vulnerabilities in the systems, i.e. the Precinct Count Optical Scan (PCOS)/Optical Mark Reader (OMR) system for the counting of votes and the Real-Time Election Information System (REIS) for the canvassing that have been adopted by Comelec. These vulnerabilities cover the different phases of the election implementation, from the proclamation of the winning bidder last May 2009 up to the proclamation of the winners in May 2010. For each vulnerable spot that CenPEG has identified, the policy study center has also proposed corresponding safeguards in order to make the whole electoral process secure, transparent, and credible.

A copy of the *30 Vulnerabilities and 30 Safeguards* study was submitted to Comelec in 2009 as well as to the Joint Congressional Oversight Committee (JCOC) on the automated elections, other groups, and individuals. Until now, however, CenPEG has not received any response from Comelec regarding its plans on addressing these vulnerable spots. (Neither have they responded to other inquiries and issues that CenPEG – along with other groups – have raised subsequently.) As the election looms, CenPEG has found that major vulnerable spots have remained so indicating Comelec's

lack of compliance with Republic Act 9369 (Automated Election Law), Comelec Request for Proposal/Terms of Reference (RFP/ToR), and other election-related laws. As a matter of fact, Project 3030 of CenPEG, a research on the AES funded by the European Union, found that the vulnerabilities are no longer limited to 30; and that many of the vulnerabilities have no corresponding safeguards thus validating CenPEG's findings.

Alarmingly, there are emerging vulnerabilities due to Comelec's decisions regarding critical features of the automated election system. Some of these vulnerabilities include: the entry of 5,000 signal jammers in the country, disablement UV security mark reading of the PCOS machine, the removal of the digital signing of the Election Returns, among many others.

This preliminary report (covering the period January 15 – March 31, 2010) is based on research, observations and participation in actual Comelec activities such as the mock elections, field tests, the simulation at the Senate, Joint Congressional Oversight Committee (JCOC) hearings on the AES, visits to the National Printing Office for the ballot printing, Comelec office, and Smartmatic-TIM's central warehouse in Cabuyao, Laguna for the election machines. This is also the result of interviews and consultations with information technology experts and participation in the JCOC hearings. Furthermore, being a comprehensive research study on the automated elections, this report also includes critiques on various Comelec Resolution, released General Instructions, and other official documents.

This report has been made possible with the support of the European Union through the European Commission delegation in the Philippines under the EU-CenPEG Project 3030.

II. FINDINGS

1. Mock Elections: Not reflective of real conditions on May 10

Two mock elections were conducted by the Comelec for the purpose of testing the capability of schools that will be serving as voting centers and the people to conduct an election with automated voting, counting, and canvassing (including transmission of results from PCOS machines to the subsequent levels of canvassing to Comelec central server). The first was held on February 6, 2010 in nine precincts spread in Luzon, Visayas, and Mindanao. The mock voting centers were in Quezon City (New Era Elementary School) and Taguig (Gen. Ricardo Papa High School and Maharlika High School) in Metro Manila, Baguio (City Camp High School and Pines High School), Cebu (Bulacao Community School and Mabini Elementary School) and Davao (Generoso Elementary School and Alejandra Navarro Elementary School).

On March 25, 2010, a second mock election was conducted at the Senate, as requested by the Joint Congressional Oversight Committee (JCOC) on Automated Elections to "look

for gaps" in the implementation process of the automation, and to provide remedies (if such are seen) through regulations by the Committee.

These two mock elections validated many of the findings or predictable outcomes made by CenPEG in 2009 about the vulnerability of the system. This is even more alarming since the mock elections were not even reflective of the real conditions on May 10 (the mock polls were conducted mostly in urbanized areas where there are long-established power and telecommunication systems) and still there were many problems encountered.

Both mock elections were conducted in controlled environments. In the first mock election held on February 6, 2010, there was pre-testing of transmission signal, briefing of the mock voters, and practicing with the machine days before the mock election. Furthermore, the mock elections were held mostly in urban places including Mabini, a semi-urban place in Cebu City. During the simulation at the Senate, the mock election was conducted inside air-conditioned rooms. Add to this, in both mock elections, the number of mock voters did not simulate the approximate number of voters for each PCOS machine on May 10. There were only 50 voters per PCOS machine in the first mock election and 100 in the second. This number is statistically small compared to the 500-1,000 voters who will cast their ballots using each PCOS machine in the actual elections. Because of the controlled environment and the number of mock voters quantitatively small compared with the actual number of potential voters per PCOS machine on May 10, the problems that arose during the mock elections will likely increase in magnitude on May 10 including queuing and actual length of time within which each voter must finish voting from registering, filling the ballot, feeding the ballot into the machine, and getting an indelible ink mark.

Despite the controlled environment, problems still arose during the mock elections. Some vulnerable spots that CenPEG had earlier identified in 2009 were validated in the mock elections. Some of these problems are:

1. Some BEIs and BOCs had difficulty keying in their passwords during the initialization of the machine; on actual election day, if the machines fail to initialize immediately, voting cannot proceed as scheduled. A delay in the start of the voting will mean that there will be less voting time, and thus less voters will be able to vote within the 7 a.m.-6 p.m. (later extended to 7 p.m.) voting time allocation.
2. It was difficult for the voters to keep their ballots secure and secret because of the ballot's length allowing it to be exposed to other voters' – and even BEIs' – eyes. The voters' right to SECRET VOTING is thus jeopardized.
3. Some voters found it difficult to understand the English instructions on the ballot and the small font; with the long time incurred at this stage, other voters will have to queue up at the polling area. Also, errors in shading (it is possible for others to accidentally shade an oval for a candidate they do not

actually want to vote) are inevitable, especially to the un-schooled and the senior citizens.

4. Some ballots in each observed precinct on February 6 were rejected/invalidated by the machine, without ample explanation being given to the voters; this indicates a possible disenfranchisement of voters on May 10;
5. There was no clear procedure for the treatment of rejected / invalidated ballots;
6. There was no verifiability of voter's choice; thus the voters did not know if the machine interpreted their ballots correctly in violation of Article 7(n) of RA 9369;

   There was an incident of failure of the closing of polls. The failure of closing of polls on election day would mean that ballots can still be fed into the machine. At this point, the possibility of unused ballots being shaded and fed into the PCOS is not remote. Likewise, if the polls don't close immediately, the transmission of ERs cannot be done on schedule;
7. Secret keys were already saved into the PCOS machine, showing clearly that it is the machine – as programmed by Smartmatic-TIM - that signed the election return and not the BEI, a violation of Section 19 of RA 9369. The Comelec had earlier been informed by CenPEG that allowing Smartmatic-TIM to generate the secret keys steals the authority that is conferred only on the BEIs and gives it – along with Comelec – the potential power to tamper with the election process;
8. Lack of BEI training on the Revised General Instructions (Comelec Resolution No. 8739) causing confusion in the conduct of the mock elections such as the giving of two ballots to one voter and the problems with keying in passwords;
9. There was no transparency during canvassing. Watchers were only able to see the "colored signal buttons" on the canvassing laptops which show if the ERs from specific polling centers are not yet transmitted, are being transmitted, or are already transmitted. Since laptops are very small, and the screen was not projected using LCD projectors, it is almost impossible for watchers at canvassing centers to watch the process, except to wait for announcements from members of the BOC; and
10. The results of manual audit in the Senate simulation did not match with the results on printed ERs, showing a discrepancy in how the machine interpreted the ballot and how a human being interprets the ballot. This is an indication that possible discrepancies in RMA on election day may also happen. That being so, how can we trust that the PCOS machines that the Comelec-Smartmatic will be using on May 10 are accurate and can really record and count the votes the way they should be counted?

Add to these, problems attending past manual elections have surfaced in the automated elections as proven during the mock elections as well as reports pertaining to padded voters' lists and statistically improbable population increases in many regions including

the ARMM which is noted for widespread election fraud. These clearly show that, contrary to its much-hyped plans to cleanse the voters' registration lists in preparation for the automated elections such have not been addressed decisively leaving the whole exercise prone to flying voters and disenfranchisements.

Kontra Daya, a multi-sectoral poll watch dog reported early March 2009 that the 50 million plus registered voters is actually padded with approximately 5 million because of double or multiple registrants in the voters' list that hasn't be cleaned yet by the Commission. Even the Parish Pastoral Council for Responsible Voting (PPCRV), Comelec's official citizen's arm discovered at least 40,000 multiple registrants in their manual checking of the voters' list. Comelec maintained its position that it has already cleansed the list, but said that they will look into the reports of various groups.

Problems with the voter's list, registration lines, and voters who voted twice were observed during the mock elections. And lastly, the 11-hour voting window will not accommodate 1,000 voters for each PCOS machine.

In CenPEG's time and motion study of the mock elections, only a maximum of 550 voters will be able to vote during the 11-hour voting window. In order to accommodate 1,000 voters on May 10 Comelec officials should extend the voting time from 11 to 16 hours or, in extreme scenarios, 20-40 hours. Comelec authorities say that voting can be extended to 16 hours but assurances that the voting machines' batteries can last for 16 hours in areas where electricity is unstable remains a question precisely because none of the PCOS machines were subjected to a stress-test in actual Philippine conditions, as the law required. Unless addressed decisively, the time constraints aggravated by possible power and transmission failures can lead to widespread voters' disenfranchisement.

2. No Source Code Review

On October 5, 2009 CenPEG filed a Petition for Mandamus before the Supreme Court (SC) to compel Comelec to release the source code for review by any interested parties or groups as provided by Section 14 of RA 9369. CenPEG was compelled to petition the SC for mandamus in order to direct the Comelec to comply with the legal requirement of releasing the source code for review based on the request of CenPEG (of May 26, 2009) and duly approved en banc by the poll body on June 16, 2009; a copy of the approval was received by CenPEG only on July 10, 2010. At that time, CenPEG had assembled at least 20 volunteers for the source code review coming from the country's reputable computer science schools (UP, Ateneo and DLSU), ICT academics and professionals, systems experts and programmers and had secured the commitments of various institutions including the UP's College of Law and College of Engineering computer science for the free use of their facilities. Methodologies, instruments, as well as laboratory design had also been planned.

Aside from the legal requirement, the review of the source code is important because it will reveal if the program that will run the machines that will count and canvass the votes is compliant with RA 9369 and the Comelec RFP/ToR and is free from manipulation. In short, a source code review is conducted primarily to verify that the system will do what it is supposed to do, that is, read the votes, tally, and transmit them properly. A proper review that can take up to four months to conduct will answer the following questions:

1. Do the various sets of instructions to be given to the PCOS correctly and accurately reflect the instructions on how the (PCOS) will recognize the voting intents of the voters and appropriately count the votes in accordance with the rules specified in our election laws?
2. Do the various sets of instructions to be given to the Consolidation/Canvassing System (CCS) correctly and accurately reflect the instructions on how the CCS will summarize the vote counts coming from various PCOS machines in accordance with the rules specified in our election laws?
3. Do the various sets of instructions to be given to the Election Management System correctly and accurately reflect the instructions on how the EMS will be used to generate specific parameters for use by each PCOS or CCS in accordance with the rules specified in our election laws?
4. Are the various sets of instructions written in a manner such that there are no vulnerable instructions that may be exploited by third parties to introduce codes designed to manipulate the outcome of the vote count or vote consolidation?
5. Are the various sets of instructions free and clear of codes designed to manipulate the outcome of the vote count or vote consolidation?

However, until now, Comelec has failed to release the source code which is in clear violation of the law. Last January 27, 2010, three months before the election, Comelec announced that it will open the source code for review, and released a nine-point guideline for interested parties to follow and adhere to. The nine-point guideline includes the submission of credentials of the source code reviewers of the interested parties, signing of a non-disclosure agreement, and submission of the methodologies to be used in the review, among others.

According to CenPEG IT consultant Lito Averia Jr., a number of the requirements in the nine-point guidelines appear to be just and fair, such as the signing of a non-disclosure agreement and the provision by the Comelec of a room where the reviewers can do their own review of the source code. However, some pointers, such as the provision of a read-only copy of the source code will constrain reviewers from doing a proper and comprehensive review, given the already restrictive amount of time left before election day. Another CenPEG IT Consultant Pablo Manalastas, PhD, agreed and said that, with the given guidelines, what the Comelec offers is thus only a code walk-through and not a review as mandated by law.

Because the code is impossible to be properly reviewed due to Comelec's restrictive guidelines, political parties and groups, including CenPEG, refused to participate. Only the Parish Pastoral Council for Responsible Voting (PPCRV) submitted their intent to conduct a code walk-through, but Comelec still has not taken action on this intent of PPCRV. Given the very limited time to conduct even a walk-through, it is now impossible for Comelec to comply with Sec. 19 of RA 9369, subjecting the election results under suspicion in the absence of a source code review. Voters will be unable to know how exactly their votes were counted and tallied.

It should also be noted at this point, that Comelec dilly-dallied with making the source code available for review by CenPEG. Obstacles were set at every stage when CenPEG followed up several times with the poll body for the release of the computer software. The obstacles included citing another provision of RA 9369 that clearly pertained to another procedure; and arbitrarily requiring the policy center to submit first an application paper, an international certification on the competence of its IT volunteers, SEC papers, and others.

It became clear, however, that Comelec could not release the source code because it was another company, the U.S.-based Canadian Dominion Systems that owns the source code. Smartmatic paid for a "License to use". In the case of the Philippine elections, Smartmatic was authorized to deploy the software binaries for use in the AES. Such, again, is in clear violation of the election law.

3. Certification by SysTest Labs and the Technical Evaluation Committee

Comelec and Smartmatic-TIM paid PhP70 million to a U.S.-based company, SysTest Labs, to conduct the international certification of the system. SysTest Labs is supposed to certify several components of the system such as the mock elections, the accuracy, functionality, and security controls of the AES software, and the successful completion of a source code review. So far, however, the only document issued by SysTest and which has been released by Comelec is the Certification of Final Trusted Build that was completed on February 4, 2010. The subject of the certification is the source code files and binary files of the Automated Election System.

The documented tests of SysTest are the basis for the certification of the Technical Evaluation Committee (TEC), mandated by RA 9369 to release the certification "not later than three months before the date of the electoral exercises." TEC, headed by Dennis Villorente came out with its certification on March 9, 2010 that states "the AES, as submitted, with full adoption of the recommended compensating controls, can securely, accurately, and properly be used by voters, boards of election inspectors, local and national boards of canvassers, and COMELEC in the May 10, 2010 National and Local Elections."

Part of the certification of the TEC is making sure that field tests and mock elections were held successfully. However, according to Engr. Villorente, while it is the task of the TEC to ensure that these tests were conducted, the Comelec and Smartmatic are the ones that set the standards in identifying whether a test was successfully conducted or not. Since the TEC plays the role of an observer and consultant, it ensures that the tests are conducted, and suggests ways for improvement depending on the results of these tests.

A successful conduct of a source code review is also a requirement for the TEC certification. On this aspect, the TEC relied mainly on the conduct of the source code review of Systest Labs, ensuring that it complied with the Voluntary Voting System Guidelines 2005 (VVSG 2005) set by the US Election Assistance Commission. Obviously, the "source code review" was not conducted in actual Philippine conditions.

In its certification released, the TEC stated that "*this certification excludes the public website, KBP server, central server, back-up central server, election system DNS server, PCOS modem firmware, and ballot production tool, which were not submitted for full certification and testing."* This differs with the provision of the law stating that the TEC should certify *"the AES, including its hardware and software component."*

Despite the non-compliance by Comelec and Smartmatic-TIM with certain provisions of RA 9369, among them the source code review, digital signing, and verifiability of voter's choice, the certification was issued by the TEC.

4. No Verifiability of Voter's Choice

Article 7 (n) of RA 9369 about minimum system requirements states that the technology must *"Provide the voter a system of verification to find out whether or not the machine has registered his choice."* Smartmatic's PCOS machine, the Smartmatic Auditable Election System (SAES) 1800 has a feature that would allow the voter to view how his/her ballot was interpreted by the machine. If the machine interpreted the ballot correctly, the voter can press the "CAST" button and the ballot will be dropped into the ballot box. However, if the machine incorrectly interpreted the ballot, the voter is given the right to press the "RETURN" button, correct possible errors in the ballot, and re-feed the ballot. This is a system of verification. However, Comelec has disabled this feature of the machine and until now has refused to use it in all of its demonstrations, voter's education, and during the mock elections. This, again, is in clear violation of the law.

In response to criticisms regarding this, Comelec has said that the post-election random manual audit is the proper instrument for verifying the votes and establishing the integrity of the election results. This, however, is clearly in contravention of the election law. When earlier asked why the system of verification was disabled, a Comelec official said "it's a waste of time."

The requirement of verification will establish whether the ballot markings done by the voter are faithfully and correctly scanned, stored, and transmitted by the voting machine. It is precisely this feature that establishes the trustworthiness and reliability of the system insofar as the voter is concerned. Correct counting begins with the reading and scanning of the voters' choice. The voter's verification and approval is needed to give him/her assurance that his/her ballots have been correctly read before they are processed for counting, transmission, consolidation, and canvassing. Unless ballots are verified by the voter, the reliability of the machine is never established thus further casting doubts on the system's integrity and on the election results.

CenPEG has consistently taken the position that while the new election system should be able to shorten the length of the election, this should not be done at the expense of the voters' right of verification, public counting, and the need for building trust on the automation system itself. Comelec prioritizes speed – in order to quicken the proclamation of election winners – over the voter's rights. This proposition has nothing to do with "modernizing the election" where it is expected that voters' rights are protected and enhanced and not restricted, as what will happen on election day.

5. No Digital Signing

Section 19 of RA 9369 states that: *"The election returns transmitted electronically and digitally signed shall be considered as official election results and shall be used as the basis for the canvassing of votes and the proclamation of a candidate."* However, in the Revised General Instructions, there is no instruction for the teacher to perform the function of digital signing.

The instruction is actually to bypass digital signing. Renato Garcia, Comelec IT Consultant, explained in a meeting that there is still digital signing which will be triggered by the iButton key. RA8792 or the ECA defines electronic signature as a mark or a procedure adopted by a person. Comelec hinges digital signing on the procedure to be triggered by the BEI with the use of the iButton key. However, there is nothing in the GI for BEIs that requires the BEI chair to execute a digital signature based on legal electronic industry standards.

This is in clear violation of RA 9369. Not only will the integrity of the election returns to be transmitted be endangered, it is also unlawful to remove the process of digitally signing the election returns before transmitting them to the canvassing centers. Removing the digital signing will, in effect, render the transmitted election results unofficial. Establishing due execution as required by RA9269 cannot be bypassed.

Rule 2 Section 1 (i) of Resolution 8804 states:

> "i) ***Electronic Transmission*** refers to the act of conveying data in electronic form from one location to the other."
>
> "q) ***Electronic document*** refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored processed, retrieve or produced electronically. It includes digitally signed documents and **any print-out or output, readable by sight or other means, which accurately reflects the electronic document**."

Section 19 of 9369 states:

> "The election returns transmitted electronically and digitally signed shall be considered as official election results and shall be used as the basis for the canvassing of votes and the proclamation of a candidate."

This shows that any data in electronic form, whether transmitted electronically or physically transported to be canvassed, as long as it is in electronic form (soft copy), is an electronic document and is electronically transmitted. This can thus be used as basis for proclamation despite its lack of proper safeguard in the process of transmission. However, this definition is a legally-twisted definition of the term "electronic transmission". Manual conveyance or hand delivery is definitely not "electronic transmission."

Great danger is posed on the integrity of the ERs that will be canvassed because while under the law only the initially "protected and secured" digitally-signed ERs should be electronically-transmitted these can now be physically transported to the canvassing center devoid of the digital signature.

Moreover, the automated election system being put in place for the May 10 polls has practically changed the rules on the transmission of electoral results, traditionally a contentious electoral issue. Since the basis of the canvass will be electronically-transmitted results based on RA 9369 and Resolution 8804 (Rules on Dispute Resolution in the Automated Election System), how will the Comelec now consider the results from manual polling that might be done in places where automation has failed?

Electronic transmission refers to the act of conveying data in electronic form from one location to the other, based on current election laws. However, Comelec has recently

announced that it is preparing for possible partial manual canvassing of votes, while asserting that there will be no nationwide failure of elections.

6. Ballots: Delays in printing, and no NPO security mark in the ARMM ballots

The printing of 50.8 million ballots was scheduled to start January 25, 2010 but actual printing started only on February 7 due to problems brought about by changing the orientation of the ballots from a vertical list to a horizontal list. Fast tracking the printing of ballots also led to the printing of ballots with a list of candidates that was not yet final. For example, Vetellano Acosta's name, a presidential candidate who was eventually disqualified, was still included, along with other Party-list groups with pending petitions for disqualification.

The RfP/ToR requires the ballots to have security markings. Comelec implemented five security markings on each ballot. However, NPO asked Comelec, as early as November 2009, to include the NPO security marking in the ballots, a feature of ballots in manual elections attesting that the ballot was indeed printed by the NPO. But Comelec has failed to implement it. Comelec decided to use UV ink instead of the 2D NPO mark. By this time, however, the ARMM ballots have already been printed without the UV mark. There is a total of 1,882,339 voters in the ARMM as of January 15, 2010.

Another concern was the estimated delay in the completion of ballot printing. A confidential Comelec internal memo issued March 1, 2010 a copy of which was obtained by CenPEG states that the printing of ballots at the National Printing Office (NPO) is on "Red Alert Status" because of delays due primarily to printers printing below capacity and the breaking down of one of four printers for at least two days. The expected daily capacity of four printers is 800,000 ballots, but according to the memo, it was able to produce an average of 650,000 only a day. In order for Comelec and Smartmatic-TIM to meet their April 25 target date of completion, they should be able to print at least 793,430 ballots a day, which is impossible given the current state of the printers. Comelec tried to solve this by purchasing another printer which became operational on April 5. Comelec and Smartmatic-TIM were able to complete printing on April 24, a day earlier than the target date.

However, with the delays and eventual rush in the printing of ballots to meet the deadline, the ballots' quality was sacrificed. For example, ballots were exposed to errors in printing, which resulted in misalignment of UV security markings. Because the UV marks were in the wrong position and cannot be properly detected by the PCOS machines, the UV mark detection feature of the machines was removed.

Comelec has also confirmed that it is printing 30 percent more ballots as a contingency measure in voting areas where manual elections will be held due to absence of transmission connectivity, power failures, and other problems. However, until now, no

guidelines have been issued by Comelec that will reconcile the differences of appreciation for counting between manual counting and PCOS counting. There are also no details on how the results from manual counting will be consolidated with the electronic election returns in the canvassing centers.

7. PCOS Machines: Disablement of UV security mark scanners

According to the ToR, *"The system shall have necessary safeguards to determine the authenticity of a ballot, such as, but not limited to, the use of bar codes, holograms, color shifting ink, microprinting, to be provided on the ballot and* ***which can be recognized by the system****"* (Item 17, Component 1-B Precinct Count Optical Scan, Technical Specifications). However, Comelec disabled the UV security mark scanner on the PCOS machines because Smartmatic-TIM used the wrong UV ink for the ballot security markings. The UV ink lacked density which cannot be detected by the PCOS machines. Comelec officials knew about this since January 2010 while conducting laboratory tests. Comelec has instead opted to use about 80,000 handheld UV lamps thus expecting the BEIs to manually scan the ballots for UV marks on Election Day. The 80,000 handheld UV lamps cost PhP 30.2million but no supplier has been identified and no public bidding conducted as of April 29, 2010.

Using the handheld UV lamp violates the ToR requirement that the machine must be able to recognize the security marking. Aside from this, it is alarming that the use of handheld UV lamp is not yet included in the Revised General Instructions and the teachers have not yet been trained to use the UV lamp. Even if the BEI is able to detect the UV markings, it is not clear or the Comelec has not indicated what figure/image will be seen as a UV mark. Further, the GI for BEIs has not been amended or a supplement not issued to instruct the BEI to perform hand-scanning. Thus, failing to perform hand-scanning is not an election offense. There are no clear indications that the UV lamps have also been tested to establish their reliability. Ironically, the use of UV lamps by the BEI to establish the authenticity of every ballot will add time to the voting process. Moreover, whether Comelec has continuity plan in case some of ballots turn out to be un-recognizable or shown to be fake through the UV lamp and hence need to be replaced, remains unclear.

8. Storage and Deployment of Machines

Based on the ToR during bidding, among the duties of the winning bidder, Smartmatic-TIM, is the storage and deployment of machines. The consortium will also assume all costs for this particular project component. The machines will be stored in the main warehouse in Cabuyao, Laguna until they are deployed to sub-hubs in different parts of the country. To secure the delivery, two of the three logistics firms that have been awarded the contract to deliver the machines have hired security agencies. Add to this, the Armed Forces of the Philippines (AFP) and the Philippine National Police (PNP) will

have an active role in securing the voting machines and other election paraphernalia as they will be under the "full disposal" of Comelec. Aside from the security agencies and the AFP and PNP, Comelec will also rely on the pollwatchers to monitor the delivery and storage of election paraphernalia.

The three logistics firms contracted by Smartmatic-TIM to deliver the machines are relatively small players in the logistics industry, according to Lito Averia and project research. These three firms - Argo International Forwarders, Ace Logistics, and Germalin – have relatively small domestic market shares. Based on the 2008 domestic cargo traffic flow statistics from the Civil Aviation Board (CAB), Argo International only placed 11th with a total market share of 0.42%; Germalin at 12th place with 0.35% market share. Ace Logistics is not among the top 30 companies of forwarders. This data is based on actual chargeable weight in freight handled by the companies.

The small size of the firms and their relatively limited networks across the country put in question their capability to deliver 82,000 PCOS machines to specific areas in the country. Add to this, in order to fulfill the delivery of the election paraphernalia, the firms will use local subcontractors to assist in the delivery and warehousing. The three firms and the local subcontractors have direct accountability to Smartmatic-TIM and not to Comelec. Furthermore, there is a higher possibility that local subcontractors may have links with local politicians or partisan groups.

9. Training of the BEIs: Delayed and Inadequate

According to the Implementation Calendar set by the Comelec in the RfP/TOR, the training of PCOS operators (members of the BEI most of whom are public teachers), and their certification will be conducted from January 20 to April 30, 2010 for areas outside the Autonomous Area of Muslim Mindanao (ARMM), and from March 11 to March 14 for ARMM areas. The actual training, however, started only on March 1, 2010, two months delayed from their original schedule. The training programs were held simultaneously in various parts of the country. Each training was conducted in two days with the first day dedicated to familiarizing the BEI members with the PCOS machine and the second day allotted for the exam to be taken by the trainees.

The one day allotted for the lecture and demonstration on the PCOS machine is deemed to be inadequate to familiarize the teachers with the machine as well as in solving potential problems they will encounter on Election Day. Moreover, according to a BEI trained in Manila, the teachers were trained only for the Final Testing and Sealing Day leaving them with no skills on the transmission of data and on how to use the handheld UV lamps. Based on the testimony of one teacher who attended the training, the BEIs do not know yet the full extent of their responsibilities. And lastly, the passing grade for the exam is only 60% which is too low for gauging the BEI members' capability to handle the voting, counting, and transmission system on Election Day.

10. Voter Education

Comelec, together with the Parish Pastoral Council for Responsible Voting and Smartmatic-TIM, claims to have started its voter education in August 2009. It used media (print, radio, broadcast, and the internet) as well as forums and demonstrations in different parts of the country to familiarize the public with the PCOS machine and "demystify" the automated election system.

The contents of their voter education manual, however, reveal insufficient information on possible problems on Election Day and the contingencies that Comelec and the public should adopt to secure the elections and the votes. In particular, Comelec and PPCRV do not educate the public about the canvassing procedures and therefore how to watch it. Their manuals also do not teach the voters how to assert their right to vote and be counted if the machine fails to accept their ballots. In terms of coverage, the voter's education does not reach parts of the country where many Filipinos have not yet even seen a computer. The voter education campaign does not address how people will become familiar and comfortable with the new technology given that many Filipinos have never touched let alone seen a computer in their lives. Introducing a new technology is not just introducing the machine – it is also about changing people's consciousness and enhancing their level of technological awareness which takes several years. In the U.S., voting machines were installed for a couple of years at malls and other public venues for voters to familiarize themselves before their final use.

11. Transmission

The site survey of Smartmatic-TIM in the latter months of 2009 revealed that only 64% of the country has connectivity while 32% have none. When Smartmatic-TIM submitted their bidding documents last year, they were working under the assumption that 90% of the country has transmission capability based on the requirements in the bid documents that Comelec provided them. The areas that do not have connectivity will have to rely on satellite transceiver to be able to transmit their election reports. However, aside from reliability using satellite might have legal implications.

According to reliable IT sources, if satellite technology is used, the data will be taken first to Hawaii, outside our country, and might stay there for a couple of minutes before it can be transmitted back. Now the question is, what is the legal implication of taking election reports including election returns outside of the country even if for just a few minutes?

12. Revised General Instructions for the BEI

The long delayed final General Instructions for the BEI has recently been released by Comelec. A scrutiny of the Revised GI reveals a lack of proper safeguards such as the

removal of digital signing. Below is a list of some safeguards that should have been in the GI:

- BEI actions should be announced to the public.
- There should be instructions on what will be done to ballots that do not have UV markings.
- There should be instructions on what will be done to voters who will not get ballots because of the lack of UV markings.
- The GI does not contain any instruction for the BEI to get the ballots at the Treasurer's Office.
- There should be more security for the back-up CF card. It is not sufficient to just place it in a small envelope that is easy to steal.

13. No Mechanism for a Proper Random Manual Audit

The Random Manual Audit (RMA) is the last line of defense against cheating or fraud in the elections that the law provides under section 29 of RA 9369: *"Where the AES is used, there shall be a random manual audit in one precinct per congressional district randomly chosen by the Commission in each province and city."* PPCRV has been accredited by Comelec to conduct the RMA for the May 10 elections. However, the independence of PPCRV may have been compromised since it is part of the Comelec Advisory Council (CAC) that has fully supported the AES despite its lack of safeguards and non-compliance with major provisions of the election law. Another problem with the RMA is that Comelec plans to conduct it only after the proclamation, which renders the RMA moot and academic given the lengthy time it takes to resolve electoral protests if discrepancies are found. The lack of attention of Comelec to the RMA, the last line of defense, is indicative of the small importance it gives to this process and to ensuring clean and credible elections on May 10.

14. Other emerging vulnerabilities

The decisions the Comelec has made in recent months point to a lack of proper and sufficient preparation for the May 10 automated elections as well as an alarming disregard for safeguards to make the automated elections compliant with RA 9369 and ensure an open, clean, and credible election. Below is a list of other emerging vulnerabilities aside from those already mentioned earlier:

- If ballots without UV markings are simply set aside and not destroyed, these can still be used for cheating especially since the PCOS UV detection feature was disabled. Thus the ballots can still be inserted and accepted by the machine. (Proposed safeguard: GI should be clear on the treatment of such ballots)
- If the statistical and audit log reports are not transmitted, there will be no basis for verifying the election results (in terms of number of voters, number of

accepted ballots, and number of invalidated ballots) and the activities conducted on the PCOS machine. It is only through the audit log report that watchdogs will see what the BEIs and technicians actually did on the PCOS machine. (Proposed safeguard: statistical and audit log reports should be transmitted to the municipal, Comelec, and shared servers)

- The back-up CF card will be kept in a small envelope of around 3x4 inches. The small size of the pack makes the back-up CF card vulnerable to theft as it can be easily put inside the back pocket or bag. (Proposed safeguard: the back-up CF card should be kept in a bigger pack that would make it less vulnerable to easy theft)
- There is no way to check the contents of the back-up CF card prior to voting day. Without this safeguard, the back-up CF card can already be pre-populated with data which can then be the data that will be transmitted at the end of voting day.
- If the technicians are under Smartmatic-TIM, from whom will they take orders during Election Day? According to law, it should be Comelec that must supervise the elections.

III. ANNEXES: SPECIFIC STUDIES

Period covered: January 15 – March 31, 2010

A. MOCK ELECTIONS (February 6, 2010)

(Based on the reports of Nadja Castillo, Ayi dela Cruz, Roda Manalac, Kontradaya, Sister Elsa Compuesto, MSM, of the Sisters Association of Mindanao, John Panem of Baguio City, and Prof. Sherwin Ona of AESWatch)

The Commission on Elections conducted its first mock elections for the May 10, 2010 national and local automated elections last February 6, 2010. They were held in Quezon City (New Era Elementary School) and Taguig (Gen. Ricardo Papa High School and Maharlika High School) in Metro Manila, Baguio (City Camp High School and Pines High School), Cebu (Bulacao Community School and Mabini Elementary School) and Davao (Generoso Elementary School and Alejandra Navarro Elementary School). The CenPEG Project 3030, AESWatch, and networks such as Kontradaya and College Editors Guild of the Philippines were able to monitor and observe the mock elections in all of the schools except in Mabini Elementary School.

Participants

The participants in the mock elections for each voting center consisted of 50 mock voters, three Board of Election Inspectors, three to four Comelec officers, and Smartmatic technical personnel. The mock voters were representative of the population except in New Era where the majority of the participants were teachers and in Ricardo Papa where 17 of the 50 voters were teachers and city hall staff because not all pre-selected voters showed up.

Aside from the participants in the actual mock elections, poll watch groups were also able to observe the proceedings although they encountered problems with the transparency of certain processes (see below). Five representatives from poll watch groups were asked to witness the voting in New Era and Ricardo Papa because the place was too crowded with the added presence of the media.

Issue 1: The confusion with the voters' list and the incident of a voter who was able to vote twice

Tension briefly erupted in Maharlika when some preselected voters discovered that their names were not listed in the Voters' List. There were also discrepancies in the names listed on the Comelec officers' Voters' List and the names in the Voters' List posted outside the polling center. This basic problem with the Voters' List that can occur on a much bigger scale in May 10 is not addressed by automating the elections.

Another problem that automation will not solve is the presence of flying voters if proper procedures are not observed by the BEI. In Maharlika, one voter was able to vote twice

after the BEI failed to put an indelible ink on her finger after voting. She tried to vote again under a different name and was able to cast her votes twice.

Issue 2: Presence of police and military inside the precinct
Aside from the participants directly involved in voting, there was a strong police and military presence in Alejandra Navarro Elementary School in Davao wherein the PNP outnumbered the voters and in Ricardo Papa High School in Taguig wherein there were 7 PNP personnel inside the classroom and not more than 20 PNP personnel one of whom was carrying a long firearm and 1 AFP personnel in General Office Attire uniform inside the school premises. The presence of the police and military in Taguig was questioned by Comelec officials but the PNP personnel explained that they were just there to observe. In Davao, meanwhile, the police was invited by Comelec to observe the proceedings.

The police and military presence inside the precincts was in clear violation of the BEI General Instructions that states that it is unlawful for any officer or member of the AFP or the PNP to "enter any polling place or stay within a radius of fifty (50) meters" except to vote.

Conduct of Mock Elections

Issue 3: Transmission was tested in some precincts the day before the mock elections
In Ricardo Papa and New Era, Comelec tested the transmission of the PCOS machine the day before the mock elections. In Ricardo Papa, voting was held on the second floor after they tested that the first floor does not have any signal.

The testing of the transmission is a necessary action that Comelec should have addressed months before in order to provide the public a realistic picture of the real conditions on the actual day of elections. Thus testing the transmission a day prior to the mock elections means that the mock elections was not conducted in real conditions since many areas in the country does not have transmission capabilities. The outcome of the transmission does not provide the public with a realistic scenario of what will occur in May 10.

Issue 4: Feeding of ballots was rehearsed the day before the mock elections
The purpose of the mock elections was to show the public that the automated elections will work in "real" conditions. However, in New Era, the ballots were fed into the PCOS machine the day before the mock elections as a form of practice for the teachers. This shows that the actual conduct of the mock elections in New Era was staged especially with most of the mock voters composed of teachers.

Initialization of machine
The initialization of machine in all precincts was finished in five minutes. No problems in powering the machine were encountered. However, there was no transparency in

Alejandra Navarro Elementary School in Davao wherein the report was shown only briefly to the public before it was sealed in a white envelope.

Issue 5: BEI improperly keyed-in password
In Baguio, the BEI typed the password twice even though s/he was holding a copy of the password. This kind of difficulty with the password might be experienced by many BEIs in May 10.

Registration starts
The registration of voters started at different times in the precincts. Some precincts such as Bulacao Community School in Cebu, City Camp High School and Pines High School in Baguio started one hour late because the pre-selected voters did not arrive on time.

Issue 6: Thumb marks were obtained from the voter prior to the accomplishment of the ballot
In Ricardo Papa, thumb marks from the voters were obtained prior to the accomplishment of the ballot which increases the risk that the voter will smudge his/her ballot as s/he is filling it out.

Voter fills in ballot

Issue 7: Average time to fill in ballot is not reflective of real conditions in May 10
The average time it took for one voter to fill in a ballot was 3 minutes. However, this is again, not reflective of the actual number of minutes it would take for the voter to fill in his/her ballot on actual Election Day. The mock voters did not need to think about their choices in the mock voting hence hastening significantly their accomplishment of the ballot.

Issue 8: Secrecy of ballot cannot be ensured
The very long ballot design made it difficult for voters to keep their ballots secret. The Secrecy Folder could not hide adequately the ballot of the voter as s/he was filling it out. In Ricardo Papa, AESWatch observer Sherwin Ona also reported that proper precinct lay-out was not observed which might result to compromising the secrecy of the balloting process.

Issue 9: Long ballot and small font difficult for some voters
Some voters, such as an elderly in New Era, complained that the font of the print on the ballot was too small and that the instructions were written in English. A senior citizen in Ricardo Papa had to bring her daughter along to help her read the ballot. This design of the ballot will make it difficult for the illiterate, elderly, and linguistic minority to fill in the ballot easily and correctly.

This difficulty with the ballot is exacerbated by the lack of assistance that the BEI extended to the voters, particularly those whose ballots were rejected due to "ambiguous marks" (to be discussed below).

According to Comelec, the ballot to be used in May 10 will be much shorter with the print written horizontally rather than vertically. However, this was not the ballot used during the mock elections nor is it the ballot used during voter's education. If the actual ballot design to be used in May 10 will not be made public soon, many voters might have a difficult time filling in the ballot on the actual day of elections.

Voter feeds ballot into PCOS machine

The feeding of the ballot into the PCOS machine took only several seconds especially for those that did not encounter any problems. However, as was expected, some ballots were rejected by the machine for various reasons.

Issue 10: Several attempts to feed a ballot and paper jamming

In Ricardo Papa, there were two incidents wherein the voter had to fill in his/her ballot more than twice. In one incident, a voter's ballot was rejected twice. The voter explained to CenPEG researcher Nadja Castillo that the BEIs thought that the reason why her ballot was rejected on the first two attempts was due to a scotch tape on the scanner which the BEIs failed to remove. When it was removed, however, and they tried to feed the ballot for the third time, the ballot was again rejected. That was when they noticed that the voter filled in double ballots or two ballots stacked together. The voter apparently thought that she was filling in one ballot and shaded the two stacked ballots one face each. To try to resolve this, the BEI took one ballot (with only one face shaded) and fed it into the machine, then returned the other ballot (also with one face shaded) to the pile of blank ballots. This was later given to the next voter who took the ballot (with a "pre-shaded" face) with no protest.

In Maharlika, the PCOS jammed twice (according to DZMM the machine jammed thrice). Two valid ballots were affected by the jamming of the machine. To resolve the problem, the machine had to be rebooted and opened twice and the technician had to approach the machine five times. However, after rebooting the machine, the ballot of the next voter also got stuck in the machine. The Smartmatic personnel again tried to fix the machine and discovered that there was a small piece of paper stuck in the feeder.

Issue 11: Ballots rejected, voter disenfranchised

There were rejected ballots in all but one precinct that were monitored by the research. In New Era, five ballots were rejected, one due to crumpling, the others due to ambiguous marks. The voter whose ballot was rejected due to crumpling complained that it got crumpled because the precinct was too crowded with people, possibly reflecting the real condition on voting day. In Bulacao Community School, two ballots were rejected, one because the voter intentionally tampered with the security markings. In Generoso Elementary School, one ballot was rejected as invalid while four

ballots were rejected in Alejandro Navarro Elementary School, both in Davao. In Maharlike, three ballots were rejected, and in Baguio, one ballot was rejected due to ambiguous marks.

According to *Smartmatic*-TIM technical support manager Miguel Avila improper shading is read as "ambiguous marks" by the machine which is then prompted to reject the ballots. According to him, "There is a configurable marking threshold that the Comelec and Smartmatic- TIM agreed on. The threshold was set at fifty percent. Meaning, if the mark did not reach the fifty percent shading of the oval, the mark will not be counted as a valid mark. We call that an ambiguous mark; Comelec and Smartmatic-TIM have agreed that the machines be configured to detect ambiguous marks." He said this configuration will allow voters another chance to correct any ambiguous marks.

This problem with ambiguous marks and the sensitivity of the ballots to crumpling and stray markings put the voter at higher risk of being disenfranchised on voting day. In the case of New Era, 10% of the ballots were rejected. If the same happens on Election Day, 10% will be a significant number of voters disenfranchised.

Issue 12: No proper mechanism for the treatment of rejected ballots

In Alejandra Navarro, rejected ballots were just folded by the BEI and placed on the side without showing to the public the rejected ballots and the reason why they were rejected. In New Era, the rejected ballots were just given to the BEI.

Issue 13: There is no verifiability of voter's choice

As is expected by the research team, there is no way for the voter to verify how the machine interpreted his/her ballot. While the majority of mock voters did not seem to mind this, one voter in New Era stated "*Ginawa ko naman yung tamang pag-shade sa bilog pero pano ko malalaman kung binasa nga ang boto ko*?" Such sentiments are sure to be repeated during the actual Election Day.

Issue 14: Failure of closing of polls

In Bulacao Community School in Cebu, the machine failed to close immediately. The BEI had to place the RF key on the button repeatedly until the machine closed.

In all other precincts observed by the group, the machines closed without any problems.

Issue 15: Secret keys are already saved into the PCOS machine

After the ER is generated, the electronic copy should be digitally signed by the BEIs using their secret keys which should ideally be contained in an external storage device. However, during the mock elections, the secret keys were already saved into the PCOS machine. The BEIs generated it by typing their passphrases. With the secret keys saved

into the machine, it is essentially the machine the signs the ER and not the BEI, which is in violation of RA 9369.

Issue 16: Lack of transparency with the ER and the audit log report
In Alejandra Navarro, the BEIs did not give a copy of the ER and the audit log report to the poll watchers for scrutiny.

Issue 17: Lack of training of the BEIs
The incident in Ricardo Papa wherein the voter mistakenly filled out two ballots and the BEI resolved it by returning the other filled ballot to the stack shows the lack of training and preparedness of the BEIs for the May 10 elections.

In Alejandra Navarro Elementary School in Davao, it was the Comelec personnel and technicians who operated the machine and not the BEIs. It was also Comelec personnel who assisted the voters feed their ballot into the machine further endangering the secrecy of the ballot.

And in New Era, the BEI failed to explain to the voters why their ballots were rejected nor did the BEI assist the voters whose ballots were rejected due to ambiguous marks.

Transmission
The transmission of results went as planned in all of the precincts observed by the research group with results transmitted to the canvassing center and Comelec Central Server within the first few minutes. Only the transmission to the KBP server took long (almost an hour, after several attempts) because the server of KBP was down. A proclamation from the Central Server was made by 12:08 noon.

However, it should be kept in mind that the precincts' transmission capabilities were tested the day before and that all, except for the school in Mabini Cebu, are in urban areas.

Canvassing level

Issue 18: Lack of transparency during canvassing
The poll watchers could not do anything but wait for announcements from the BOC or look at the canvassing computer screens briefly regarding the transmission of ERs and the results. There was no LCD projector for the public to view the activities in the canvassing computers and requests by Sherwin Ona of AESWatch to have the results posted online were not answered by the MBOC in Taguig. With this lack of transparency, public participation in the electoral process is further compromised.

Issue 19: Use of laptops as tools for the consolidated canvassing
The use of laptops as tools for the consolidated canvassing is seen by the Dela Salle group of Sherwin One to be a very dangerous practice that can lead to possible

tampering of results of the incoming PCOS transmission; dumb terminals (e.g. without keyboards) should instead be used for this purpose.

Issue 20: BOC did not know how to type the password
In Davao City, the BOC Chair did not know how to input and verify the passwords of other members of the BOC showing clearly a lack of training of the personnel who will run the elections in May 10.

Over-all assessment

While it did take only 5-8 minutes for the voter to register, fill in his ballot, and feed it into the machine, and the whole process from opening of machine to transmission took only 1 hour and 20 minutes up to 2 hours and 20 minutes, these do not approximate the actual amount of time that these tasks will be accomplished on May 10. First of all, only 50 voters participated in the mock elections in each precinct when it should be 1000 voters, to approximate the actual conditions on May 10. Secondly, the voters did not need to think about their choices, thus they filled up the ballot very quickly. Add to this, transmission capabilities of the precincts were tested and incidences of practicing with the machine a day prior to mock elections were reported clearly showing that the mock elections were still conducted in controlled conditions.

And yet, given the time it would need to accomplish the ballot (approximately 5-8 minutes for ordinary voters and 10-12 minutes for elderly voters which are conservative estimates given the reasons cited above), it is anticipated that the allotted 11 hours for voting will not be enough to accommodate the number of projected voters in a clustered precinct. If 50 voters took 1 hour and 4 minutes to finish voting, the 11-hour voting window will only accommodate 550 voters.

The chokepoint is actually with the BEI – service time takes about 1 min and 30 secs. Filling out the ballot becomes a chokepoint only if voters spend more than 15 minutes. Given the BEI service time, to process 1,000 voters will require 25 hours with a constant arrival rate of voters. At 80% turn out, this means that the polls will have to be open for 20 hours.

It is also disturbing the PNP and AFP personnel presence was prominent in several precincts. This is in clear violation of election laws and would sow fear among voters should this happen on Election Day.

There are also still problems with the lack of training that the BEIs and BOCs have. The mock elections clearly show that they are still unprepared for the switch to automated election system. And the GI lacks instructions on the treatment of rejected ballots and the transparency of the process of verifying the reason for the rejection of ballots.

Technical problems still hound the PCOS, from the unfriendly ballot to problems with feeding the ballot into the machine. Such problems will occur on a larger scale in May 10 and would disenfranchise thousands of voters.

Comelec and Smartmatic dismiss these technical problems as voter's education problems. They however, have yet to launch a massive and far reaching education campaign that will reach all corners of the country in order to address this problem. Furthermore, dismissing it as a voter's education problem will not address the fact that many voters will still be disenfranchised. And this will not address the problem of the secrecy of the ballots with the current design of the ballots.

And lastly, there is a general lack of transparency with the automated elections. There is no verifiability of voter's choice, there is a lack of security of data with the secret keys saved into the machine, and no LCD projector for the scrutiny of the public of canvassing results.

Comelec actually introduced a vulnerability with the issuance of Bid Bulleting No. 10 which specifies that the winning bidder will generate the keys. In principles of digital signing, a trusted third party infrastructure is used for signing. Users of the infrastructure actually generate their own keys to the private key private. The problem with the vendor generating the signing keys is with people on the vendor side who are vulnerable to being compromised could provide an opportunity to tamper or manipulate the election results or generate/manufacture election reports and signing the same with valid keys. The tampered or manufactured data cannot be detected.

B. JCOC MOCK ELECTION at PHILIPPINE SENATE

Prepared by Ayi dela Cruz, March 25, 2010

How the mock election was conducted

The mock elections held by the Joint Congressional Oversight Committee (JCOC) on the automated elections at the Senate last March 25, 2010 was conducted to simulate actual Election Day. It was an end-to-end testing, from voting to transmission.

Two precincts were placed side by side representing Sorsogon City (Voting Center I) and the municipality of Donsol (Voting Center II) in Sorsogon province. Each voting center had 100 voters including senate staff, Senator Francis "Chiz" Escudero, Comelec chairman Jose Melo and Tita De Villa of PPCRV.

Meanwhile, the different levels of canvassing centers were assigned in selected rooms inside the Senate. (See appendix)

A voters' information desk was also set up outside the voting center with PPCRV Chair Tita De Villa manning the desk herself, together with other PPCRV officials.

Selection of Voters

Voting participants were selected by the JCOC through convenience sampling. Participants were a mix of residents from around the Senate area, students, Senate employees and others. They were contacted by the JCOC and asked if they want to participate in a mock election for them to be able to learn how to vote. The age of voters ranges from 18 to 75 years. They are then assigned a name from an actual list of voters from the province of Sorsogon.

Voter Registration

The "voters" then proceeded to verify their precinct number from the list of voters posted on the wall. Once they have gotten their respective precinct numbers, they went to the Voter's Help Desk to affix their signature and thumbprint on their names on the list of voters. They were then given a stub containing a sequence number to present upon entering the voting precinct for them to get a ballot (the ballot is only given inside the precinct), or attend the Orientation, in case they have not.

Voters' Orientation

The orientation wass done by batch and was given by a Anna De Villa Singson, PPCRV voters' education specialist. The most common questions from the voters concern over-voting and under-voting.

Below are key points discussed during the orientation:

1. Look up your name on the voter's list. If you do not find your name, go to the voter's help desk. Get a sequence number.
2. Go to the precinct and give your sequence number and name to the BEI. The BEI will check your name and photo on the computer database. If your registration does not have a photo, present a valid ID. A valid ID is one which contains your photo; the cedula is not accepted.
3. The BEI will then give you the ballot. The ballot is 25 inches long. The front contains the positions and candidates for the national level. The back has names and positions fo rhte local level.
4. How do you vote? Shade the inside of the oblong, or if you've been watching TV, the *bilog na hugis itlog* (circle shaped like an egg). This is the correct way of doing it [points to visual aid].
5. Do not put any other mark on the ballot. In other mock elections, the people doodle on the ballot. They put flowers, smileys or butterflies. Do not do that. Do not mark the bar code. Do not fold the ballot. The machine might read these marks as votes and your ballot might be rejected.
6. There is only one ballot per voter. You only get one chance to vote, so if possible, bring a list of candidates that you will vote for. Question, if I commit a mistake and put an X over it, will that be okay? No.
7. Do not overvote. For the position of president, choose only one. Same for the vice-president. For senator choose only twelve. If you vote more than twelve, your vote for senator will not be counted. Why will it not be counted? If you choose more than twelve, the machine cannot determine which twelve to count, so it will not count your votes for that position.
8. What if you undervote? That is okay. You votes will be counted.
9. What will you use to shade the ballot? Comelec will provide a marker. Can you bring your own markers? No.
10. Go to the PCOS machine where an IT-enabled BEI will check your signature. Will you show your ballot? No, the ballot is sacred. The PCOS machine is like a fax machine; it's as big as a laptop computer.
11. The "ballots cast" screen will show how many votes have been cast. After you put in your ballot, it will add one to "ballots cast." If, before you cast your vote, the "ballots cast" screen shows 20, what should be shown after? [21]. If you see 22, or 23, or any other number, notify the BEI. As a citizen, it is your right and responsibility to guard the election process.
12. When you are done voting, return the secrecy folder and marking pen to the BEI, and the BEI will mark your finger with indelible ink. Not returning the marker is an election offense.

Findings

1. Venue for the JCOC mock poll does not reflect real conditions

The March 25 simulation was not held under real conditions and all processes from voting to canvassing were all done inside one building. Thus, the outcome is not reflective of what will actually happen on Election Day.

a) Mock voters were only 100 per precinct. On actual Election Day, there will be a maximum of 1,000 voters.
   - The BEIs and Comelec were not able to devise or test crowd control mechanisms needed for handling almost 1,000 voters per precinct.

b) Far-flung areas are not represented
   - Coverage and effectiveness of Voters' Ed in far-flung areas not tested
   - Transmission infrastructure in far-flung areas and reliability of backup transmission equipment such as satellites (BGANs and VSATs) were not tested
   - Power capabilities in far-flung areas and reliability of batteries and generators were also not tested

c) Size and layout of clustered precinct in the Senate is not the same as size and layout of clustered precincts on actual Election Day, which will definitely be smaller (average classroom size).

2. 11-hour voting window still not enough

Time and Motion Study in one clustered precinct (Sorsogon city) revealed that in a controlled environment such as the Senate, where the BEI is well-prepared, voters and observers were not disorderly, and there were no technical glitches, it would take approximately 1 hour and 30 minutes for 100 voters to finish casting their votes. That means that with the 11-hour (or 660 minutes) voting period on Election Day, under these ideal conditions, only 750 voters can be accommodated.

Actual cases of voters timed upon approaching the BEI for identity verification (signature and thumb mark, short instruction on how to fill out the ballot, receiving of ballot, secrecy folder and felt tip pen), until vote is successfully cast:

1	Male, mid-40s	10 minutes
2	Male, youth/apx. early 20s	9 minutes
3	Male, apx. late 50s	6 minutes
4	Female, mid-30s, middle-class (perceived)	8 minutes
5	Female, apx. 40s, senate staff	13 minutes
6	Male, disabled (in wheel chair), apx. 50s, middle-class (perceived)	7 minutes
7	Female, apx. 60 years old (elderly)	9 minutes
8	Female, apx. 70 years old (elderly)	14 minutes

9	Senator Chiz Escudero	6 minutes
10	Chairman Jose Melo	5 minutes
AVERAGE		**8.7 MINUTES**

Actual case of voter timed while in queue until vote is successfully cast:

	Queuing time	**Voting Time**	**Total**
1	2nd in queue (1 minute)	9 minutes	10 minutes
2	3rd in queue (3 minutes)	5 minutes	8 minutes
3	5th in queue (5 minutes)	5 minutes	10 minutes

The average time to fill in the ballot was not reflective of real conditions in May 10 because the mock voters did not need to think too hard about their choices in the mock voting. The names in the ballots were not actual candidates' names, hence significantly hastening their accomplishment of the ballot. Ballots used are also in the old format. New ballot format has not yet been tested on voters.

3. Lack of BEIs training on the Revised General Instructions for BEIs

A voter was disenfranchised because BEI was not familiar with the revised protocol on how to handle rejected ballots.

A voter who used x marks on her ballot instead of shading the ovals was instructed to feed her ballot in different orientations into the machine four times. And when ballot was still rejected, that was only time that the BEI checked her ballot and saw the x markings. The BEI should have instructed the voter to check for ambiguous marks or other stray markings.

In the Revised GI for BEIs, rejection of ballot is allowed only four times. If ballot is still rejected on the fourth try, it will be invalided, placed in an envelope, and will not be counted. In this instance, therefore, the voter was not given a chance to correct the shadings in her ballot, which should have been done after her ballot was rejected for the first time.

4. Results of manual audit do not match with results on printed ERs

There was a discrepancy of 1 to 3 votes per elective position in once clustered precinct with 100 voters. This is a big number if projected on Election Day with 1,000 voters per clustered precinct and more than 70,000 clustered precincts nationwide. This may translate into thousands of vote discrepancies per elective position.

In the Donsol precinct, there was discrepancy in the manual audit for the position of president. Candidate number 55 had one less vote in the manual count than in the ER. It was later found that there was a mistake in the manual count.

Also, in the Provincial Governor position, 2 candidates were found to have 1 vote discrepancy each.

Differences in outcome of machine counting and manual counting of votes point to differences in appreciation of votes by humans and by the machines.

Offhand, the discrepancies may be due to some over-votes on particular elective positions (meaning voter casted more votes on an elective position than what is required). If a voter over-voted in a particular office, votes in this office will not be counted by the machine. However, some of these over-votes may have been randomly counted and included in the tally by the machine. Also, markings on the ballots made by some voters which, to the BEIs and volunteers conducting the manual audit, should not have been counted were still counted by the machine. And markings that for BEIs are legitimate markings may not have been counted by the machine.

Actual case: Researchers who participated in the manual audit saw a ballot marking where the voter shaded only the outer part of the oval. The BEI who was reading out the votes, showed this to the tallying group where it was argued whether to count this as a vote or not. One PPCRV official said this should be counted by the machine, because this is a valid mark since the machine did not recognize this as an “ambiguous mark”. However, another PPCRV official said that this is not a valid mark since only the outline of the oval was shaded and therefore the machine was not able to read the mark. It was decided to set aside this ballot in case there will be discrepancies with the manual tally and ER. However, due to the numerous discrepancies, it was no longer traced which ballots were erroneously ready either by the machine or the manual audit group. One PPCRV official even that said this is “normal” and within the “acceptable” error. It was also confirmed that the Comelec has not yet released the GI on manual audit.

Tracing the discrepancy is even more difficult since the ER is not programmed to print how many voters did not vote and how many over voted in a particular office.

5. There is still no verifiability of voters’ choice

One of the causes of discrepancies in the manual and electronic count is the absence of verifiability of votes.

The argument on whether the machine counted the oval marking made by one voter during the manual audit should have been first verified by the voter himself if the verifiability function is available.

Moreover, while voters' education emphasizes on filling out the whole oval, there are still voters who will make mistakes on Election Day, especially those in far-flung areas who have not been reached by voters' education.

6. Risk of smudging the ballot

The thumb marks were obtained from the voter prior to the accomplishment of the ballot, which increases the risk that the voter will smudge the ballot while filling it out.

The BEI also applied indelible ink to the voter before feeding the ballot into the machine.

However, based on the revised General Instructions for BEI (Comelec Resolution No. 8686, March 4, 2010), putting of indelible ink and thumb marking shall only come AFTER the voter has fed his ballot into the machine.

> ***SEC. 36. Manner of voting,*** - Voting shall be conducted in the following manner:
>
> a) The voter shall, using a ballot secrecy folder and the marking pen provided by the COMELEC, fill his ballot by **fully shading the oval** beside the names of the candidates and political party participating in the party list system of representation of his choice; (***Renumbered)***
>
> b) The voter shall then approach the PCOS, insert his ballot in the ballot entry slot and wait until message "CONGRATULATIONS. YOUR VOTE HAS BEEN REGISTERED." appears on the screen. The BE1 shall monitor the PCOS screen to make sure that the ballot was successfully accepted. Thereafter, the voter shall return the ballot secrecy folder and marking pen to the chairman; ***(As revised)***
>
> c) The **BE1** shall apply indelible ink at the base and extending to the cuticle of the right forefinger nail of the voter, or any other nail if there be no forefinger nail; ***(Renumbered)***
>
> d) The voter shall affix his thumbmark on the corresponding space in the EDCVL; and ***(Renumbered)***
>
> e) The voter shall then leave the polling place. ***(Renumbered)***

Actual case: A ballot was rejected at the Alin, Donsol precinct. Upon the BEI's examination of the ballot, it was found that the barcode at the side of the ballot was smudged with ink.

7. BEI did not affix digital signature

The BEIs were not required to enter the digital signature before the electronic transmission of results, following instructions from the Revised General Instructions for BEIs because the secret keys were already saved in the PCOS machine instead of in an external storage device. This is in violation of RA 9369 because with the secret keys already in the machine, it is essentially the machine that signs the ER and not the BEI.

> ***Sec 22 of RA9369: Electronic Returns***
>
> "The election returns transmitted electronically and digitally signed shall be
> considered as official election results and shall be used as the basis for the canvassing of votes and the proclamation of a candidate."

8. BEI was assisted by pollwatchers

In some instances, pollwatchers were performing some of the BEIs functions as defined in the Revised General Instructions, such as reloading the machine with a new roll of thermal paper when it ran out of paper. In another instance, someone from Smartmatic-TIM was giving instructions to the BEI on how to use the modem during transmission. As per Revised GI for BEIs, only the BEIs and technicians are allowed to have access to the machine during the voting process.

9. Use of laptops for consolidating and canvassing votes

As what was also pointed out during the February 6 mock elections, use of laptops as tools for the CCS, instead of dumb terminals (e.g. without keyboards), is a dangerous practice that can lead to possible tampering of results.

Summary of Findings

While the mock elections held at the Senate is said to be "successful" - transmission was smooth (all under 2 minutes to the different servers) and few ballots rejected (4 out of 100 in Alin, Sorsogon precinct) – it is premature to assume that this reflects a successful May 10 elections.

Ultimately, the condition at the Senate actually makes it the least ideal venue for a simulation. It is the total opposite of the set up in public schools, especially in far-flung areas.

a) Ample security
b) Trained BEIs (even then, there were still signs of inadequate training)
c) Only 100 voters per precinct
d) Organized crowd control with cords to guide the crowd (there is "holding room" for the rest of the voters while waiting for their turn at the precincts)
e) Air-conditioned and with spacious halls as voting precincts
f) Done in the presence of high officials (Comelec, PPCRV, Senate) and the media
g) No transmission issues/ strong signal area

Thus, given these conditions, a true stress-test of the system did not happen. There were no opportunities for the BEIs, voters and poll watchers to anticipate and carry out continuity plans that may be brought about by, for instance, having 1,000 voters, or setting-up of the BGAN or VSAT in case of a transmission problems. In short, this was not a simulation at all.

Recommendations

1. As what have been our call since the February 6 mock elections, there is still a need to hold another mock elections that with simulate actual conditions on May 10, 2010.
   a) 1,000 mock voters per precinct
   b) far-flung areas are represented (with issues in literacy, transmission, etc.)
   c) in actual classroom and polling area setting

2. The Comelec should also come out with proper and comprehensive rules for the conduct of the Random Manual Audit (RMA). This should include resolving discrepancies in manual and electronic appreciation and determining the acceptable error for discrepancies.

   Moreover, the discrepancies in counting of votes by machine and BEIs/volunteers through the manual audit only revealed that the RMA should be conducted prior to Proclamation. It is only logical to double-check the electronically counted votes by doing a manual audit before proclamation.

   In this regard, CenPEG, together with other citizens' groups and experts in the field of mathematics and statistics, are preparing a proposal that would cover for the appropriate methodology, as well as guidelines for the conduct of the RMA.

C. STUDY ON THE SOURCE CODE REVIEW
(Prepared by Jaime Hernandez IV, Project 3030 IT Research)

Introduction: What is a Source Code Review?

Creating software takes a lot of effort. Generally, the process involves designing the software, coding, and testing and debugging. The final step, testing and debugging, is an almost non-stop process. The software, usually at this time in its beta stages, undergoes several testing procedures, whereupon any glitch encountered is acted upon. The source code review comes at this stage of software development. The source code is scrutinized part by part to test for accuracy, security, performance, and documentation, to name just a few.

The source code is the human-readable version of the program running on the machine. For the source code to be read by a machine, it has to be converted into machine-readable format. This conversion process is called compiling, and the program that converts the source code into machine readable format is called a compiler. Just as there are versions of the programming language used to write the source code, there are also versions of the compiler.

A source code review is conducted to assure that the software produced is of quality standard. Quality may be viewed differently depending on which perspective one adopts. Kitchenham and Pfleeger discuss five views of software quality[1] as follows:

1. Transcendental View: quality as a characteristic that is recognizable but difficult to define.
2. User View: perceives quality as fitness for purpose
3. Manufacturing View: quality is understood as the extent to which the product meets its specifications.
4. Product View: quality is viewed as tied to the inherent characteristics of the product.
5. Value-Based View: quality, in this perspective, depends on the amount a customer is willing to pay for it.

The source code review may be conducted as a check on the software quality from a manufacturing and product point-of-view. The source code review, however, is not the sole basis for appraising the quality of software. Several software quality models have been defined for the purpose of assessing software quality. One model, the ISO 9126, defines six categories of quality characteristics: functionality, reliability, usability, efficiency, maintainability, and portability.[2] The source code review is one tool that tests against these categories of quality, or any defined categories of quality, by looking at and testing the actual program code.

Why Conduct a Source Code Review of the Automated Election System?

Normally, when one buys software, one need not look at the source code under the premise that the manufacturer has tested the software and had it undergo rigorous testing procedures before the software is sold. This is the popular practice when the software is bought—and therefore not *open source*. Open source software is software distributed for free. More importantly, the source code of said software is available for the public to download, review, or modify. This results to the software having several versions, and these versions are released by different groups or individuals. These new versions are improvements or customizations of the existing or latest software. For example, a bug in the software may be reported to the open source community, and a version which has the glitch resolved is released. Ultimately, the users of the system, the open source community, benefit.

For the 2010 Automated Election, a source code review is conducted primarily to verify that the system will do what it is supposed to do, that is, read the votes and tally them properly. This means checking to see that the system itself does not cheat, is free of errors that may cause it to register votes incorrectly or to malfunction, and has security measures set in place as to prevent hacking of the system and safeguard against any malicious software.

Although it is assumed that the seller, in this case Smartmatic-TIM, has done the necessary audit of the software before it is sold, and that the buyer, Comelec, has scrutinized the system and tested it to see that it meets requirements set by them (quality from a User View), a source code review is still necessary for the citizens to check the quality of the system. This is important if the chosen election system must establish its credibility to facilitate the exercise of the citizens' sacred right to vote. This, after all, is the point of using an automated election system. A change of voting procedure is carried out to improve on the current election process—mainly in terms of speed of counting and ease of voting—while maintaining the credibility of the voting process. A change into the automated election system without a source code review by the public defeats the purpose of using electronic machinery in the elections.

Aside from verifying that the system works, a source code review is done "to check that these programs conform to Philippine election laws, like the Omnibus Election Code BP881, AES Law RA8436, AES Law Revised RA9369, COMELEC 2009 TOR/RFP, and the COMELEC 2010 General Instructions, and are properly written election programs as specified in US-EAC-2005-VVSG, where the provisions of 2005VVSG do not conflict with our local laws."[3]

On January 23, 2007, Congress passed Republic Act No. 9369[4] (RA 9369), otherwise known as the New Automated Polls Law. RA 9369 establishes the need to ensure a transparent Automated Election System through a source code review. Section 14 states that

> "*Once an AES technology is selected for implementation, the Commission shall promptly make the source code of that technology available and open to any interested political party or groups which may conduct their own review thereof.*"

This source code review is different from the independent source code review carried out by an international entity for the Technical Evaluation Committee certification. Section 11 of RA 9369 states that the Technical Evaluation Committee:

> "*shall certify, through an established international certification entity to be chosen by the Commission from the recommendations of the Advisory Council, not later than three months before the date of the electoral exercises, categorically stating that the AES, including its hardware and software components, is operating properly, securely, and accurately, in accordance with the provisions of this Act based, among others, on the following documented results:*
> *…*
> *3. The successful completion of a source code review;*"

Comelec Guidelines on the Conduct of Source Code Review for the 2010 Automated Election System

A source code review takes several months to finish. That is why as early as September 2009, CenPEG together with other concerned stakeholders has already submitted a Petition for Mandamus to the Supreme Court to release the source code for review as mandated by the law. Comelec, has however, failed to respond to the Mandamus. And it is only last January 27, 2010, three months before the elections, that it released its guidelines for what it calls a source code review.

The following are the guidelines set by the Comelec in the conduct of the public source code review for the 2010 Automated Election System:[5]

1. Entities interested in conducting a source code review must signify their interest in writing for approval of the COMELEC and submit to COMELEC the credentials of their source code reviewers.

2. Entities approved by COMELEC shall sign a nondisclosure agreement before they are allowed to conduct the source code review.

3. Entities which will conduct the source code review shall submit to COMELEC the methodologies they propose to use.

4. COMELEC shall provide a secure and enclosed location/facility for the conduct of the source code review; and all entries and exits into the facility shall be properly recorded.

5. A read-only copy of the source code shall be provided on secured COMELEC workstations in the secured location/facility.

6. No copies of the source code or any part thereof maybe taken out from the secured location/facility.

7. No electronic devices of any kind, including but not limited to laptops, mobile phones, cameras, USB drives and other storage devices, shall be permitted inside the secured location/facility.

8. Each entity that conducts a source code review shall submit a report to the COMELEC after the review period.

9. The COMELEC reserves the right to issue supplemental guidelines in the conduct of the Source Code review.

The first guideline is set to ensure that only competent individuals get to review the source code. It would be a waste of time and other resources to allow the source code to be reviewed by those who do not know how to conduct a source code review.

The second guideline defeats the purpose of a source code review of the Automated Election System. The purpose of a source code review is to assure the public that the system is honest, is free of critical errors, and is secure. Since only individuals knowledgeable in software engineering and audit may conduct the source code review, the rest of the citizens rely on these experts, who are also a part of the voting public yet independent of Comelec, to report on the credibility of the system. It is therefore imperative that those who conduct the source code review share their findings to the public. The NDA addresses only the techniques used in the software which may not be disclosed to the public. The findings, however, are not covered by the NDA.

Guidelines number five and seven simply do not allow for a source code review. When reviewing software, one needs software analysis tools, which are run on a computer. A read-only version of the source code cannot be tested by these tools. Software, especially one as large as that of the Automated Election System (reported as 400,000 lines of code), cannot be tested by any other means. If the source code “review” proceeds in the manner stated by the Comelec guidelines, there will be no review but a walkthrough.

Other restrictions provided for in the guidelines do not allow a thorough source code review. The guidelines that the review be conducted in a Comelec facility and that no copy of the source code may be taken out of the facility restrict the software auditors to conducting the source code review with very little time. Reviewing source code takes time, and if the review is to be done properly, ample time must be given. Moreover, Comelec's interpretation of the phrase "for implementation" is flawed since it did not consider IT practice definition. In the IT practice includes customization and operationalization. Comelec thus created a legal barrier by separating customization from operationalization. Going by Comelec's interpretation of the phrase, could the Comelec have erred by choosing a system that is not ready for implementation, turning the contract into partly a customization contract? This is worth exploring as among the possible sins of the Comelec.

In his blog, Dr. Pablo Manalastas talks about the source code review in light of Section 14 of RA 9369. He highlights that "Section 14 of RA9369 requires that 'Once an AES technology is selected for implementation' COMELEC has to make the source code 'available and open' so that the interested political parties and groups 'may conduct their own review thereof.'" [6]

"*Once an AES Technology is selected for Implementation ....*" The AES technology was selected for implementation on July 14, 2009 when Comelec signed the contract with Smartmatic-TIM. The source code of the PCOS, CCS and EMS should have been made available to interested groups on that date. This, however, was not carried out by Comelec. For example, CenPEG requested for a copy of the source code in May 2009. In an *en banc* resolution dated June 16, 2009, Comelec decided to grant the source code to CenPEG, but Comelec later reversed itself in a letter dated August 26, 2009 signed by Atty. Rafanan. In the letter, Atty. Rafanan interprets the law as "Once an AES technology is selected, AND customizations are implemented, and the resulting system is tested and certified." The law clearly does not have those additional requirements.[7]

"*... make the source code ...available and open ....*" Comelec has made the source code available through the source code review, despite its restrictions. However, making the source code "open" invites a whole new discourse as to the meaning of the word. Does "open" mean simply free for the public to study, or open in the sense of open source software, as described by the General Public License? The open source interpretation provides a more encompassing definition of open: in this, as open for further development by the programming community. However, if the more limited view is taken, the public is still provided with a right to study the software without the restrictions of a non-disclosure agreement. It is therefore the minimum requirement for Comelec to make the source code available for review free from the restrictions of guidelines 5, 6 and 7.[8]

" '*...political parties and groups may conduct their own review...*' What 'own review' means was most eloquently expressed by Supreme Court Justice Antonio Carpio, during

the pleadings in the Harry Roque versus COMELEC-Smartmatic case, in which he said, 'the COMELEC has to give the political parties the source code, so that they can bring them home, and study them.' A review by interested political parties and groups cannot be done in a COMELEC-Smartmatic-controlled environment as provided for in the COMELEC guidelines, since COMELEC-control of the review process is antithetical to the concept of independent (own) review by political parties and groups.' "[9]

The SysTest Labs Certification

Section 11 of RA 9369[10] states that the Technical Evaluation Committee (TEC)

> "*…shall certify, through an established international certification entity…that the AES, including its hardware…is operating properly, securely, and accurately….*"

The international certification entity chosen by Comelec to do the documented tests as the basis for the TEC certification is SysTest Labs, Incorporated. According to the profile posted on their website, "SysTest Labs is an internationally accredited information technology company that offers a full range of quality management, and software performance testing services and products. In addition, SysTest Labs offers digital branding consulting and licenses innovative tools for digital brand information and reputation management. Headquartered in Denver, Colorado USA, with global assignments, the SysTest Labs team of technologists and domain consultants deliver on the company's commitment to provide responsive, quality-driven solutions."[11]

SysTest Labs, Inc. was founded in 1996. In a letter dated October 28, 2008, the National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) suspended the accreditation of SysTest.[12] This was done based on an on-site assessment visit in March 2008, findings from the EAC, and observations made during an October 2008 monitoring visit.[13] On October 29, the EAC issued SysTest a Notice of Intent to Suspend,[14] following the suspension by NIST NVLAP. On October 31, SysTest sent its response to EAC asking EAC to "reconsider its position."[15] On that same day, SysTest was suspended by EAC "for failing to comply with program requirements."[16] Specifically, the suspension was imposed because SysTest lacked documented procedures and uses untrained personnel in its review process. SysTest Labs, Inc. was reinstated by the NVLAP in a letter dated February 26, 2009.[17] EAC lifted the suspension on March 5, 2009.[18]

RA 9369 provides that the certification issued by the international certification entity should contain the following documented results:[19]

"*1. The successful conduct of a field testing process followed by a mock election event in one or more cities/municipalities;*
2. The successful completion of audit on the accuracy, functionally and security controls of the AES software;