(What the Filipino people should know about the Smartmatic PCOS that was proven to be deficient with admitted program errors remaining uncorrected. The use of automation technology without the license from the real software owner, Dominion voting Systems, looms in the coming May 2013 elections with the DVS terminating its licensing agreement with Smartmatic, last May 23, 2012. An ongoing legal battle between Smartmatic and DVS filed in September 2012 in the chancery Court of Delaware, USA reveals the core issue at the heart of the PCOS problem: that the election technology used in May 2010 was not fully functional, had programming errors, with the technology owner accusing Smartmatic of not complying with international standards, a validation of studies by Filipino IT experts and social scientists as early as 2009. The ongoing battle of citizens' watchdogs and the Filipino IT community for the integrity of the vote and accountability in automated elections remains integral with the fight for the Freedom of Information --the right to know-- by the public.)
I. The Automated Election System (AES)

1) What is the Automated Election System (AES) for Philippine elections?

The AES for Philippine elections is mandated by Republic Act (RA) 9369. RA 9369 amends RA 8436, entitled "An Act authorizing the Commission on Elections to use an automated election system in the May 11, 1998 national or local elections and in subsequent national and local electoral exercises, to encourage transparency, credibility, fairness, and accuracy of elections, amending Batas Pambansa Blg. 881, as amended, RA No. 7166 and other related election laws, providing funds thereof and for other purposes"; "to use an automated election system or systems in the same election in different provinces, whether paper-based or a direct recording electronic election system as it may deem appropriate and practical for the process of voting, counting of votes and canvassing/consolidation and transmittal of results of electoral exercises" a system using appropriate technology which has been demonstrated in the voting, counting, consolidating, canvassing, and transmission of election results, and other electoral process.
SEC. 1 of RA 9369: It is the State policy to ensure free, orderly, honest, peaceful, credible and informed elections, plebiscites, referenda, recall and other similar electoral exercises by improving on the election process and adopting systems, which shall involve the use of an automated election system that will ensure the secrecy and sanctity of the ballot and all election, consolidation and transmission documents in order that the process shall be transparent and credible and the results fast, accurate and reflective of the genuine will of the people.

2) Under the poll modernization law (RA 9369), why does the country need to automate its elections?

Automating the election, lawmakers said, will eliminate clerical, human intervention-related errors. Other reasons: The conventional manual process is too long and tedious. It takes almost two months before national positions are proclaimed; to remove conditions for dagdag-bawas or wholesale cheating in manual elections.

3) What are the requirements of a credible, secured, and reliable automated election system (AES)?

The Automated Election System Watch (AES Watch), through a committee of IT, business, and management experts came up in 2009 with its System Trustworthiness, Accountability, and Readiness (STAR) Card to comprehensively assess and rate the implementation of AES primarily by Comelec and Smartmatic-TIM. The STAR Card listed 20 items of concerns rated as Pass=3; Qualified Pass=2.5; Warning=2; Danger=1; Fail=0.

a. System set-up (Will the AES be ready for full implementation?)

- Timely delivery of machines
- Quality of machines
- Technology certification
- Availability of transmission facilities
- Deployment of machines
- Physical security of machines
- Precinct-specific ballots
- Resource inventory at voting centers
- Adequate general instructions
b. Internal security (Will the AES have the necessary safeguards to prevent fraud?)

- Source code & its review
- Verifiability of voting and results
- Secured transmission of results
- Initialization of machines
- Random Manual Audit of vote counts

c. Personnel training and voters' education (Will the teachers and the voters know exactly what to do on election day?)

- Training of election personnel
- Stakeholders education & training
- Precinct assignment voters

d. Contingency planning

- Continuity plan
- Electoral protest mechanism
- Alternative election system

4) **According to the law, who are responsible for making the AES successful?**

**Government:** Comelec Project Management Office together with system-integrator Smartmatic counterparts; Comelec Advisory Council; Technical Evaluation Committee; DOST-certified IT-capable BEIs; Board of Canvassers; Joint Congressional Oversight Committee (JCOC) on AES; Armed Forces of the Philippines-Philippine National Police; and other state agencies.

**Others:** International Certification body; election watchers; media such as the Kapisanan ng mga Brodkaster sa Pilipinas (KBP); Partish Pastoral Council for Responsible Reporting (PPCRV), and the National Movement for Free Elections (NAMFREL); Political Parties and Candidates.

5) **What is the role of the other sectors in the conduct of AES?**

**Other sectors/stakeholders** mandated by the Constitution and other laws: the civil society community, NGOs, citizens' watchdogs, media, institutions, and the general public.
Their role: 1) right to participate in the electoral exercise as well as in policy- and decision-making; 2) they represent the sovereign will of the people and government emanates from them; 3) RA 9369 gives CSO and other “interested parties” the right to review the election source code, monitor the conduct of elections including the RMA, conduct dialogs with Comelec and related agencies, participate in Congress hearings including proposing amendments to existing laws, and file election protests; 4) to protect the right to suffrage, right to public information and transparency, non-interference by foreign entities, as well as to fair, honest, and credible elections they have the right to hold all government agencies and officials accountable for misdeeds with the actions to include going to court and calling for impeachment.

6) When was the AES first implemented?

The first AES was implemented in ARMM elections in 1996 and then in August 1998. There was an attempt to fully automate the national and local elections in 2004 but the Supreme Court stopped the implementation. The 2007 midterm elections was not automated due to lack of time. The May 10, 2010 presidential elections was the first to be automated.

II. How was the automated election system conducted in 2010?

What were the activities – as well as critical problems and issues - on election day (May 10, 2010) and after? Were these problems and issues addressed by Comelec and other concerned agencies?
<table>
<thead>
<tr>
<th>Phase</th>
<th>Activity / Sub-activity</th>
<th>Issue</th>
<th>Comelec</th>
<th>Appraisal of Comelec Action</th>
</tr>
</thead>
</table>
| Election Day | Election materials inventory; Booting of PCOS & signing in; Zero results printing; Declaration that poll is open for voting; | Technical problems of booting and signing in by BEI in several clustered precincts; Documented scanned votes already displayed on the PCOS before start of voting as in Biliran. | 2010: The system was a “resounding success!”  
2011: The system was a “qualified success!” | No technical report was done with accompanying documents released to the public.  
Documents explaining the nationwide problems should be disclosed to the public.  
Comelec and Smartmatic contend that the problems were expected of a new system since “no technology is perfect anyway.” |
<p>| Voting period | Voting period                                                                          | Massive disenfranchisement due to 1-blank ballot                                                                                   | The old 5 precincts-per clustered precinct-configuration has no                                                                              | The kilometric queues on election day were the best argument                                                          |</p>
<table>
<thead>
<tr>
<th>Voting period</th>
<th>per voter rule; voter authentication took too long; PCOS breakdowns (documented cases)</th>
<th>scientific basis. It was more of a cost-based decision (at what point it will be less costly than DRE). No serious queuing study and simulation were done to get a picture of how the voter lines will behave on election day and arrive at the optimum number of PCOS units.</th>
<th>that the sizing method (to determine number of PCOS units needed) was utterly wrong. It resulted in “voluntary” voter disenfranchisement due to the long waiting time. The inefficient voter identity verification step aggravated the situation further.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voter authentication &amp; identity verification</td>
<td>The Voter Registration System, a 9-year-old project which has cost at around PhP4bn, is still inefficient and incomplete</td>
<td>Comelec is so passionately biased toward the automation of the voting / canvassing processes giving less priority to the voter registration system, a project which started as far</td>
<td>Equal priority must be given to these two core and mission-critical functions of the Commission to remove the very visible messy dysfunction we saw in May 2010 between</td>
</tr>
</tbody>
</table>
back as April 2003 and which to date is still a work in progress

them. If we simplify the fundamental requisites of a trustworthy election we will arrive at only three commandments (simpler and less number than those for getting to heaven):
1) fairness (one vote per qualified voter),
2) privacy or secret ballots (votes known only to the voter), and
3) accuracy (votes are recorded as intended and counted as recorded).

Due to this messy Voters Registration System commandment #1 was most likely violated
<table>
<thead>
<tr>
<th>Ballot issuance</th>
<th>PCOS-driven fake ballots detection feature not available; automatic fake ballot detection mandatory feature did not work; work-around solution using hand-held UV scanners was ineffective.</th>
<th>Smartmatic was allowed to use used printers for printing the ballots. This caused failure in placing an effective solution on the ballots that will be detected by the PCOS automatically upon feeding of the ballots.</th>
<th>The automatic fake ballot detection feature is a MUST since any human-driven detection option will not be strictly carried out by the BEIs as what happened. Most likely fairness was violated.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual voting (shading)</td>
<td>Voter privacy was compromised due to the length of the ballot; other voters can easily see one's votes.</td>
<td>The possibility of a privacy compromise caused by the long ballot did not even come to the minds of the Comelec implementers.</td>
<td>Voter privacy or vote secrecy is a basic right of the voter and was compromised by Comelec.</td>
</tr>
<tr>
<td>Ballot submission to PCOS</td>
<td>Vote verification by voter prior to submission to PCOS, a mandatory</td>
<td>Comelec is so worried about the possible long queue that might form if the voter is given a chance to review the votes recorded by the PCOS which is a</td>
<td>Voters did not have a chance to review the votes recorded by the PCOS which is a</td>
</tr>
<tr>
<td>Queue management</td>
<td>No real and scientifically-based time and motion study of the entire voter identification and voting process was done. The 5 old precincts clustering decision was made via the seat-of-the-pants method (or what will be cheap enough to hurdle the DBM budget scrutiny if PCOS is used).</td>
<td>chance to verify whether his votes were recorded correctly that is why it allowed Smartmatic to deactivate this very important machine feature.</td>
<td>violation of the AES law. Worse, its absence removed the check that will verify the accuracy of the PCOS. A violation of accuracy – a minimum system requirement.</td>
</tr>
<tr>
<td>Execution of close of voting procedures; Shift to post-voting mode;</td>
<td>Printing of 8 ER copies</td>
<td>Comelec allowed this despite the clear intent that the ERs will be posted at the precinct wall for 48 hours after closing of polls. This will require the PCOS to have an external wider printer which Smartmatic/Dominion's proposed solution does not have.</td>
<td>Due to this unmet requirement Comelec should have disqualified Smartmatic but it did not. Instead, our election system was made to fit to the solution of Smartmatic, not the other way around. This lessened the transparency of the election conduct. This violated fairness and accuracy.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Printouts of the ERs (only 3.5-inches wide and very, very long) are too small when these are required to be posted on the precinct's wall and remain there for 48 hours after polls closed for the public to see and record.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital signing</td>
<td>The absence of a real and industry-accepted digital signature for</td>
<td>Comelec allowed a machine signature - an utterly unacceptable</td>
<td>Its absence compromises the entire election's integrity.</td>
</tr>
<tr>
<td>Transmission of results</td>
<td>Transmission of the ERs did not follow the mandatory hierarchical sequence and direction thus opening them to possible fraud.</td>
<td>Comelec allowed unrestricted transmission sequence and direction thus violating with impunity this mandatory protocol. Transmission was done to whichever had an open link at the time of transmission.</td>
<td>The correct hierarchical transmission protocol of first to the city/mun server was not followed with Comelec's approval; we did not know if the PCOS were transmitting first to a rogue server somewhere where results can be doctored or the central server itself also served as the rogue server. It is 1,634 times more</td>
</tr>
<tr>
<td>Transmission to the city/municipal consolidation server FIRST</td>
<td>The correct hierarchical transmission protocol of first to the city/mun server was not followed with Comelec's approval; we did not know if the PCOS were transmitting first to a rogue server somewhere where results can be doctored or the central server itself also served as the</td>
<td>difficult to coerce /coopt people manning one server site than 1,634 sets of people in 1,634 sites (the number of cities and municipalities). Transparency was clearly violated here.</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>To the central/KBP servers subsequently;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Printing of 22 additional ER copies;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Back-up &amp; shutdown of PCOS</td>
<td>Rogue server. It is 1,634 times more difficult to coerce people manning one server site than 1,634 sets of people in 1,634 sites.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>There are valid grounds that the CF card is not a Write-Once-Read-Many (WORM) storage medium thus opening the possibility of tampering either the results or the ballot configuration and other serious fraud.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comelec allowed this despite being a mandatory requirement which intended for a CD-R or DVD-R recording medium. The Smartmatic/Dominion proposed solution did not have either an internal or external CD/DVD drive.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>We clearly saw the CF card mess that happened 5 days before election day and on election day itself. Had Comelec adhere to the technical specifications these could have been prevented. Transparency again was a victim here.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Election materials inventory;</td>
<td>Precinct report writing;</td>
<td>The Chain-of-Custody of sensitive components (ballots, ballot boxes, CF cards, PCOS units, etc,) of the system was not secure enough to assure that it is not broken anywhere in the chain. Worse, recounts started only 10 months after election day, so much time to fraudulently tamper the ballots to match the ERs.</td>
<td>The Chain-of-Custody of sensitive components (ballots, ballot boxes, CF cards, PCOS units, etc,) of the system was not secure enough to assure that it is not broken anywhere in the chain. Worse, recounts started only 10 months after election day, so much time to fraudulently tamper the ballots to match the ERs.</td>
</tr>
<tr>
<td>Re-packing of PCOS and accessories;</td>
<td>Preparation for RMA if the precinct is subject to RMA;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initialization of city/municipal servers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Consolidation at the city/mun servers;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital signing</td>
<td>The absence of a real and industry-accepted digital signature for the ERs and COCs was a very, very large security hole; anything can be done on the results by anybody who gains access to these results.</td>
<td>Comelec allowed a machine signature - an utterly unacceptable decision for nowhere in the world and the IT industry can a machine signature qualify as a true digital signature.</td>
<td>Its absence compromises the entire election's integrity.</td>
</tr>
<tr>
<td>Transmission to central/KBP servers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initialization of central server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consolidation at central server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canvassing at Comelec Center &amp; Joint Congressional Canvassing Center</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The shockingly wrong tally of the nationwide total votes (150+ million in the Comelec Canvassing server and 250+ million in the Joint Congressional Canvassing server were ignored by these two bodies; this is an obvious technical error.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The shockingly wrong tally of the nationwide total votes (150+ million in the Comelec Canvassing server and 250+ million in the Joint Congressional Canvassing server were ignored by these two bodies; this is an obvious technical error.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>This is a BUG of terrible possible consequence which could have been detected had a proper independent source code review was allowed. The large number as per industry practice) is supposed to be the so-called system choke point (the point for the maximum number of ballots that can be counted set as a parameter of the system). Why were these two parameters set at 3 and 5 times the number of registered voters? Given a turnout of 40 million, where did the 110+ million and 210 million plus extra ballots come from</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Comelec echoed Smartmatic's excuse that the wrong tally was a result of application error.
<p>| Post Election | Random Manual Audit (RMA) | The RMA was completely wrong due to the wrong sampling method plus the samples are not representative of the election contests that were audited; given such, no defensible statistical conclusion can be gleaned from the expensive effort thus defeating the fundamental purpose of the law provision for transparency. | The RMA was completely wrong due to the wrong sampling method plus the samples are not representative of the election contests that were audited; given such, no defensible statistical conclusion can be gleaned from the expensive effort thus defeating the fundamental purpose of the law provision for transparency. | Comelec is NOT prohibited from improving on the law provision for RMA. Yes, it tried to improve the provision by gearing for 5 samples per district instead of one per law requirement. But the sampling used was completely wrong, hence, the samples were not representative of the domains audited. Ergo no useful or valid conclusion can be made from the RMA results. It ended up as just an expensive and wasteful made-for-media theatre of zero audit value. |</p>
<table>
<thead>
<tr>
<th>Proclamation</th>
<th>Proclamations were not effected as carefully as they should be resulting in protests numbering bigger than in past manual elections.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protests</td>
<td>Protests were in effect futile for the recounts were done 10 months after election day, more than time enough to lose the audit value of the results.</td>
</tr>
<tr>
<td></td>
<td>Bottomline, the 2010 AES during its use on election day and after became a black box infested with so many worms which ate its integrity, security and transparency.</td>
</tr>
</tbody>
</table>
III. Monitoring and assessment of the AES from May 10, 2010 – present

1) Why is monitoring and assessment important in the implementation of the AES?

Especially because it is a new election process with its full-blast implementation in the May 10, 2010 synchronized national and local elections, the AES should be subjected to rigorous monitoring and assessment.

Monitoring and assessment are important in order to ascertain how the AES was implemented - from preparations for the May 2010 elections, how it performed on election day, as well as post-election. Assessment is also vital in establishing whether implementation is compliant with the election modernization law (legal); follows the IT standard requirements such as security, trustworthiness, accuracy, auditability, and reliability (technical); and ensures secret voting and public counting, transparency and accountability (management).

An important aspect of the assessment is to validate the AES' goal of electoral reform particularly in minimizing if not entirely eliminating fraud as well as enhancing electoral democracy.

2) Who are mandated by law to conduct the assessment/probe of the AES?

The government bodies that are mandated by law to conduct the assessment are: Comelec, Comelec Advisory Council (CAC), and the Joint Congressional Oversight Committee (JCOC) on the AES. Congress (both the House and Senate) through its concerned committees is also mandated to probe into the conduct of the AES in aid of legislation.

In its report on “The Conduct of the Automated 2010 National and Local Elections” released only on March 7, 2011, Comelec dubbed the May 2010 AES as credible and successful. However, it downgraded its claim of “resounding success” to ”qualified success” later. The report of CAC (June 2010) described the AES as “not a perfectly executed exercise” but, “despite the mistakes committed by Comelec and Smartmatic-TIM” it “ultimately did work.” However, since the AES has too many problems that need to be solved, it recommended
to Comelec not to exercise the option to purchase the Smartmatic-TIM election system for the May 2013 elections.

The House Committee on Suffrage and Electoral Reforms (CSER) in its June 2010 report called its assessment of the AES “a mixed success”: “Automation showed no substantial advantage. On the local level, our assessment is of profound unease.” On the other hand, the JCOC on AES is mandated by law to review the automated polls within one year and recommend whether to use the same technology or a new one. But it convened finally after 2 ½ years only on Nov. 21, 2012. No assessment was ever made until Congress adjourned for the May 2013 polls.

3) What other agencies and groups were involved in the monitoring and assessment and what were their findings?

Citizens' watchdogs, organizations, and institutions that were actively involved in the monitoring and assessment included: the Automated Election System Watch (AES Watch), a broad multi-sectoral group composed of 45 organizations; the Center for People Empowerment in Governance (CenPEG); National Movement for Free Elections (NAMFREL); Philippine Computer Society (PCS); and DLSU-College of Computer Studies. Others were the Philippine Computer Society, Consortium of Christian Organizations for Rural-Urban Development (Concord through Healing Democracy); People's International Observers Mission, observers from the Global Filipino Nation, Asian Network for Free Elections (ANFREL), Carter Mission, Global Filipino Nation, former Comelec Chair Christian Monsod, and others.

4) What major findings and conclusions (or specific highlights) were made by these groups in the monitoring and assessment of the May 2010 AES?

AES Watch: The major concerns raised by AES Watch through its STAR Card were strongly validated by the actual experience in implementing the AES. The glitches, errors, and deficiencies observed throughout the country during the May 2010 elections clearly highlighted the flaws in the setup and internal security of the automated system, as well as the inadequacies in personnel training, voter's education, and contingency planning. Problems and issues encountered at the various stages of the election process, from voting and counting to canvassing and proclamation, have been recorded/documented in the reports of print and broadcast media,
the hearings of the Committee on Suffrage and Electoral Reforms of the House of Representatives, the findings of the Forensic Team constituted by the Joint Congressional Canvassing Committee to examine certain PCOS machines, and the testimonies of various election stakeholders. (*Post-Election Report of AES Watch: Recap and Validated of the STAR Card Assessment of the Preparations for the May 2010 Automated Elections, October 2010*)

*CenPEG*: There was a high incidence of technical hitches, blunders, voting procedural errors, and other operational failures throughout the country during the May 10, 2010 automated elections. As The CenPEG Report reveals, these can be attributed to the lack of safeguards, security measures, as well as timely and effective continuity/contingency measures (software, hardware, technologies, and other system components) that proved damaging to the accuracy, security, and reliability of election returns. Lacking these vital mechanisms, the automated election system (AES) that was harnessed for the May 10 polls was vulnerable not only to various glitches and management failures but also electronic cheating including possible pre-loading of election results. The Comelec is called upon to disclose all election documents – public information – to test and validate its claim of election “success” and debunk allegations of electronic fraud – all for the sake of public interest and voters' rights. (*The CenPEG Report, December 2010*)

*NAMFREL*: The preoccupation with new technology and speedy counting to impress the public came at the expense of greater transparency and accountability of the system... In spite of the automation of the voting process, traditional forms of electoral fraud such as vote buying; ballot capturing; use of minors in the campaign as well as in vote buying; threats, intimidation, and violence; and non-observance of secrecy and privacy during voting, remained rampant. (*Terminal Report, July 10, 2010*)

*Joint Forensic Team* (Final Report to Congress' Joint Canvassing Committee, June 10, 2010): “…The published hash code (in the Comelec website) is not the same as the extracted hash code”; “no digital signatures in the PCOS machines, contrary to the claims of Smartmatic”; “the PCOS machine contains a console port”; (the Team upon testing) “was able to connect an ordinary laptop computer to the console port of a PCOS machine”. (The Joint Forensic Team, led by Atty. Al Vitangcol III, examined 60 PCOS machines found in the house of a Smartmatic technician in Antipolo, Rizal after the May 10, 2010 elections.)
Christian Monsod, former Comelec Chairman: Our automation was mass-produced in one step, was not really pilot-tested satisfactorily, and was provided by a supplier who had no extensive experience in the technology and seemed to be also learning while it was being implemented. (“The 2010 Automated Elections – An Assessment,” Nov.9, 2010)

Philippine Computer Society (PCS) report on the Biliran fraud case: “There were highly questionable instances where the probability of fraud may have been perpetrated using the PCOS machines ...(based on) the audit trail of the PCOS machines and the computer audit trail of the Municipal Board of Canvassers (MBOC). …There were inconsistent protective counters displayed by the PCOS machines.”

Asian Network for Free Elections (ANFREL): “Secrecy of the ballot was virtually impossible...The operation of PCOs machines encountered numerous technical glitches, ranging from minor ones that lasted for a few minutes, to others that led to suspension of polling for hours. Delay and failure of the transmission of the elections results was widely reported.”

Carter Center (U.S.): “Review of the AES's source code was limited to an on-screen presentation conducted under the auspices of COMELEC. Concerned that such a review was inadequate to identify potential problems, many watchdog groups chose to forgo participation and were unable to review the code at all....(There was) significant curtailment of the right to vote by secret ballot in the 2010 elections...(Comelec should) conduct pre-election testing in a real-world and set at an earlier date in order to ensure adequate time to correct any issues identified.

Healing Democracy: The May 10, 2010 election was no different from previous fraudulent, anomalous, and violence-ridden polls in the country. Like in previous elections, Comelec should explain for the technical glitches, transmission failures, as well as incidents of fraud and violence taking place across the country. These election irregularities were vivid in Lanao del Sur. (Testing Democracy: The 2010 Automated Elections in Lanao del Sur, Dec. 2010)

People's International Observers Mission (PIOM): “In focusing on the machines, the Comelec lost the people. The elections were not peaceful or violence-free. Neither were the elections fair nor honest.”
Global Filipino Nation (GFN, election observers’ team): “…Events put to question the authenticity, integrity, confidentiality, veracity and accuracy of the vote counts in the ERs. The dark cloud rose from disabling critical, legally specified security features, particularly relating to the digital signatures. Thus, no one (both perceived winners and losers) can be sure whether the vote results are true and correct, and reflect the real will of the Filipino people. Accordingly, the Election Observers Team of GFN challenges the legitimacy of the election results.”

IV. Accountability

A. How were these major findings and conclusions addressed by the responsible agencies?

Pressed for transparency, Comelec under its new head held dialogs with election stakeholders led by AES Watch. Contrary to claims that it welcomed strong policy recommendations to correct the Smartmatic-TIM AES program bugs and other vulnerabilities in the final analysis Comelec refused to adopt the legally-mandated minimum system requirements such as source code review and digital signature and still exercised its “option to purchase” the PCOS machines for use in 2013. Under its new membership, the Comelec Advisory Council (CAC) welcomed demands for reforming the automation system and recommended the non-purchase of the PCOS machines. Its recommendations were, unfortunately, thumbed down by Comelec.

The Supreme Court (SC) in a Sept. 21, 2010 landmark decision directed the Comelec to release the source code for review by CenPEG and other election stakeholders. The review of the AES 2010 source code was never held due to restrictions imposed by the Comelec that made an independent, scientific, and rigorous review by IT experts impossible.
As expected, the technology provider insisted that its system was sound and boasted to the whole world about its “election success” in the Philippines. Facing persistent demands from citizens' election watch groups, Congress' election-related committees held hearings on electoral reform. As a whole however the lower House endorsed the use of the Smartmatic-TIM system for the 2013 elections. Only dogged follow-ups by AES Watch made the JCOC to convene finally in November 2012. But the assessment of the 2010 poll automation was never clearly part of its agenda.

B. How were these major findings and conclusions addressed by other election stakeholders?

Under its old leadership, the accredited citizens' watchdog, PPCRV, as expected stood for the re-use of the Smartmatic-TIM system in the 2013 elections and never indicated receptiveness to proposals by various citizens groups including its own ground-level volunteers in the provinces to either reconsider the 2010 PCOS machines or make the technology provider accountable for the errors committed.

On the other hand, since Day 1 after the 2010 elections, AES Watch and its affiliate groups along with other watchdogs lobbied for several amendments for enhancing RA 9369, held dialogs with Comelec, CAC, Congress, DOST, TEC, and other agencies, and the convening of JCOC. In cooperation with UP, it organized the first Filipino IT for Election (FIT4E) national conference in June 2011 where key IT groups, practitioners, academics, researchers, U.S.-based IT scholars, and multi-sectoral groups resolved to make election technology inclusive by tapping the expertise of Filipino IT—a resolution that was backed, at least in principle, by Comelec commissioners.

Likewise, AES Watch and affiliate organizations, for three years, pressed for Congress through its election committees to review the May 2010 election automation and probe into the accountability of the election manager and technology providers. Similarly, several bills were proposed to ensure compliance with the election law. In April 2012 individual conveners and members of AES Watch petitioned the SC for a temporary restraining order against Comelec's option to purchase the Smartmatic machines.
V. Preparations for the May 2013 mid-term elections

A. What are the critical problems and issues regarding the preparations for the May 13, 2013 elections?

1) Legal – Lack of compliance with provisions of law, like (1) the use of digital signatures to sign the election returns and certificates of canvass and (2) review of the AES source code by interested political parties and groups.

2) Technical – Use of CF cards is insecure. A write-once-read-mean storage medium was specified in the Request for Proposal for the automation of the 2010 elections. CF cards will be used again in 2013, in violation of COMELEC's defined requirement. CF cards can be transplanted with new data.

3) Management – Considering that the same number of PCOS machines will be deployed for the May 2013 elections, clustering of precincts will be maintained. COMELEC has to prepare for more voters per voting precinct, perhaps assign more BEI members for voter verification.

B. Are the critical issues and problems being addressed by Comelec?

The critical issues are not being addressed properly or are largely ignored. Just like in 2010, CF cards will be used again for 2013. The controversial machine-generated “digital signature” will be used again.

The July 24-25, 2012 “mock elections” held by Smartmatic at the lower House revealed a 97% accuracy rating which is lower than the required 99.995% rating. The low accuracy translates to 600 errors out of 20,000 ballot marks (the law mandates only 1 out of 20,000). The deficiencies and inaccuracies of the Smartmatic PCOS system were exposed again – but were belittled by Comelec - during the Feb. 2, 2013 “mock elections” which resulted in machine breakdowns, paper jams, transmission delays, and counting discrepancies.

The system that will automate the May 2013 mid-term elections has no certification by the international SysTest Labs, Inc. in the absence
of approval by the technology owner, Dominion. Comelec said they will use the voting system designed for the aborted 2011 ARMM election which is regional unlike the 2013 mid-term elections with thousands of elective positions at stake. Comelec Chairman Sixto Brillantes also announced recently there will be no source code review – the second time when this vital legal requirement will not be complied with.

C. Based on these problems and issues, what is expected to happen in the coming May 2013 elections?

Trustworthiness, reliability, accuracy, and security among others are issues that need to be addressed. While the trusted build activity has been performed (on Jan 10, 2013), the input to the trusted build process, which is the source code of the AES, has not been reviewed by any interested political party or group. If the source code cannot be trusted, how can the output (the executable code which will be loaded in the PCOS and CCS machines) be trusted?

Further, the trusted build process covered only three sets of software. The PCOS software was not subjected to the trusted build process.

The COMELEC has been awfully silent on this issue which arises from the complaint filed by Smartmatic against Dominion Voting Systems, the owner of the PCOS technology supplied by Smartmatic-TIM.

D. If not resolved, what will be the impact of these problems and issues on the voters and on the integrity of the May 2013 elections?

On May 23, 2012 the real owner of the AES system used in May 2010 terminated its licensing contract with Smartmatic. A subsequent lawsuit filed before the Delaware chancery court revealed and validated the weaknesses and vulnerabilities of AES 2010 including the non-compliance with IT standard practices. The license issue is critical as Dominion Voting Systems can probably sue COMELEC and/or the Philippine Government for using unlicensed software for the 2013 Midterm Elections.
E. Why is the real digital signature, among other minimum system requirements, not being complied with for 2013?

Comelec's position in 2010 is that while RA9369 requires signing election reports (from the PCOS and CCS) with digital signatures, the law does not identify who will sign said reports. In 2010, Comelec implemented what it referred to as "machine digital signature". Comelec further argues that electronic signature is recognized and defined by RA8792 and the definition is in two parts:

a) Where a signer adopts an electronic mark (could be any of the characters or combination of said on a computer key board, a photo, an email address, video stream, audio stream, etc)

b) Where a signer adopts a process that enables independent verification and authentication of an electronic signature.

The second part of the definition is closest to what a digital signature is.

This was contested by IT groups during the CSER Hearings at the House following the May 10, 2010 elections for the following reasons:

1. Comelec erred by considering only RA9369 to the exclusion of other election-related laws. RA9369 is an amendatory law, amending among others RA8436 and BP881. Nothing in RA9369 expressly repealed the provisions of BP881 where it mandates the members of the BEI and BOC to sign the ER and COC/SOV/COCP respectively.

2. There is no law that recognizes the legality of a "machine digital signature".

3. Digital signature as a technology implementation of electronic signature that enables independent verification of the owner of the digital signature and independent authentication is recognized by Ra8792.
VI. What have been main problems in the implementation of the Election Modernization Law or the Automated Election Law (RA 9369) since 2008?

1. Lack of transparency by the premier election manager in the country, the Commission on Elections (Comelec) in dealing with various groups of citizens' election watchdogs, Filipino IT community, research groups and other stakeholders when it comes to ensuring safeguards for security, accuracy and reliability of the chosen technology in the automated election system (AES) used for elections.

   1.1 The right to know and access public information on the AES has become an exclusive domain of only a few favored or “approved” individuals and/or groups;

   1.2 The Filipino IT community on the whole continues to be excluded and treated as second class to foreign provided technology and know-how.

2. Inconsistent and varied interpretations of provisions of the Poll Automation Law (RA 9369), among which are the following:

   2.1 Source Code Review
   2.2 Use of digital signature
   2.3 Voter verification
   2.4 Use of storage devices
   2.5 Other technical provisions like accuracy
   2.6 Pre-tested technology
   2.7 Certification and role of TEC (Technical Evaluation Committee)
   2.8 Role of the CAC (Comelec Advisory Council)

3. Major implementers including the Comelec and its major citizens' arm accredited for major technical tasks like conducting random manual audit (RMA) of the system lack knowledge, competence, and appreciation of the technical complexities.
4. Safeguards (and therefore, non-compliance and violations of the laws, TOR, agreements and contract) to ensure security, accuracy and reliability of the system are conveniently set aside or disregarded and made as excuses to give way to “lower cost,” “lack of time,” and “better alternative to manual (defined as “fraudulent”) elections.”

5. Sovereignty in running the elections is compromised when the implementers rely too heavily on a foreign technology provider which does not own the operating license of the technology. *(Note: the case between Smartmatic (technology provider in the Philippines vs Dominion Voting System (PCOS technology owner) remains unsettled in Delaware, USA since it was filed in September 2012.)*

Because of these, VOTE buying is no longer a major problem in automated elections. With the lack of major safeguards in the hardware and software components of the system, the problems in PILAHAN (long queues), BILANGAN (inaccurate counting), at BENTAHAN (not just vote buying but program system buying) are emerging as modern-day problems in election. If left unchecked, automated election forms of cheating like CF card buying, PCOS machine buying and transmission jamming plus the clustered precinct long queue-delaying tactics will prevail alongside traditional forms of cheating, wholesale fraud and violence.

VII. Is there anything yet to be done to salvage the wrong or correct the mistakes and ensure against fraud generated by a problematic automated election system if Comelec persists in using the provided technology?

With only two months to go (since publication of this Primer) before Election Day, the Comelec decided not to conduct anymore Mock Elections against the advice and request of the JCOC and AES Watch last February 6, 2013 for “confidence building” after the humiliating
humiliating February 2 Mock Elections. With major PCOS errors still uncorrected and no source code review done by political parties and interested parties as prescribed by law, the people are left to pursue all course of actions necessary to a) assert the rule of law, b) ensure that the elections push through, c) the voters' right are not violated, d) teachers' duties and rights as BEIs are protected, and e) the integrity of the vote through automation is maintained.

Based on Chairman Brillantes' public statements, automated elections with Smartmatic as technology provider, will proceed as scheduled. As the premier election manager, the Comelec must allow stakeholders, especially political parties and election watchdogs equal access to the following MINIMUM information during election day:

1) Printed precinct audit logs
2) Printed MBOC (municipal board of canvassing) audit logs
3) Continuing public website (as provided for in the law) where the canvassed votes in the national server should be posted
4) Random Manual Audit immediately after elections conducted by a competent group
5) Electronic Transmission Results

This should be contained in new Comelec Resolutions and General Instructions since only the copy of the Election Returns (ERs) are provided in RA 9369 and the outdated Omnibus Election Code as documents to be made accessible to dominant and minority political parties. All the above mentioned data are important for political parties and watchdogs to know in order to gain confidence and trust that the system used is really secured, accurate, and reliable or compliant with minimum requirements of the law, as claimed by the provider and Comelec.

Pollwatchers and voters alike should prepare for the worst. What happened during the February 2, 2013 mock elections involving only a few PCOS machines and staged-managed with ill prepared “voters” and actors' names in the ballots that did not simulate the real conditions on Election Day, has provided only a glimpse of the actual scenario come May 13, 2013. Aside from the usual kits, Watchers should equip themselves NOT only with skills on how to shade and how to cast the ballot into the PCOS, but more with detailed knowledge of the vulnerabilities of the PCOS machines and the environment of the clustered precincts. For cheaters, ignorance is bliss. For enlightened voters and watchers, ignorance is a crime.
The right to suffrage is the people's sovereign right to elect officials upon whom they confer the authority to serve the public responsibly, transparently, with accountability, and on a full-time basis. For this reason, it is imperative that the electoral process is credible, trustworthy, reliable, and accurate in serving as the instrument of the people's will.

However, given the learning lessons of the first automated elections, the lack of transparency and accountability in the system, its implementers, and oversight bodies as well as the persistence of traditional fraud which automation itself has not effectively addressed – ensuring the electoral process fair, democratic, and reliable rests on the vigilance of the people.

Automating the election is fine – but it should comply with the law and the high standards of IT and election management. While we continue to push for a reliable technology, we should be alert on the fact that modern technology's capability to eliminate fraud, whether traditional or electronic, remains to be validated.

As AES Watch has always consistently advocated, voter education and poll watching should focus not only on the external features and operations of the AES but more critically on its internal systems. Vigilant watching should as well monitor the Comelec, the foreign technology provider, and other principal agencies and implementers of poll automation as well as the election cheats. There is no substitute for vigilance and in safeguarding our freedom.
MGA DAPAT BANTAYAN BAGO MAG-ELEKSYON

HINDI EKSKYAVENING TELECON NA ETTO ANG PASPAKALAM ASI LAMAT NG DATA SA ARAW NG ELEKSYON.

PROBLEM BA YUNI EH, OB MAGSAYAW.

NO INTERNET CONNECTION!!

IKA-10000 VOTERS ANG NAGHIHINTON ISANG PRESIDENTIAL CANDIDATE.

MAGLABAN KAYA ANG BOTO KO!

TAY BAWAL NA ANG MANGSOPYA.

AND NA NGA BA YUNI PASSWORD KO?

SAHIBIN MO NA YUNI PASSWORD HA?

RAKET PO MAY SABOT NA TONGB IBINIDAGONG KING BALOTA SA AKEN?

AYAW NO KURD ZAPAG MO NA LAFE SA KOOL.

MAHINA ANG SIGNAL DITO.

MAHAYAN!

AYAW MAG-START... WALA ATANG EVENTED?

NABELANG KAYA ANG BOTO KO!

TAY BAWAL NA ANG MANGSOPYA.

AND NA NGA BA YUNI PASSWORD KO?

SAHIBIN MO NA YUNI PASSWORD HA?

RAKET PO MAY SABOT NA TONGB IBINIDAGONG KING BALOTA SA AKEN?

AYAW NO KURD ZAPAG MO NA LAFE SA KOOL.

MAHINA ANG SIGNAL DITO.

MAHAYAN!

AYAW MAG-START... WALA ATANG EVENTED?

NABELANG KAYA ANG BOTO KO!

TAY BAWAL NA ANG MANGSOPYA.

AND NA NGA BA YUNI PASSWORD KO?

SAHIBIN MO NA YUNI PASSWORD HA?

RAKET PO MAY SABOT NA TONGB IBINIDAGONG KING BALOTA SA AKEN?

AYAW NO KURD ZAPAG MO NA LAFE SA KOOL.

MAHINA ANG SIGNAL DITO.

MAHAYAN!

AYAW MAG-START... WALA ATANG EVENTED?

NABELANG KAYA ANG BOTO KO!

TAY BAWAL NA ANG MANGSOPYA.

AND NA NGA BA YUNI PASSWORD KO?

SAHIBIN MO NA YUNI PASSWORD HA?

RAKET PO MAY SABOT NA TONGB IBINIDAGONG KING BALOTA SA AKEN?

AYAW NO KURD ZAPAG MO NA LAFE SA KOOL.

MAHINA ANG SIGNAL DITO.

MAHAYAN!
Launched on Jan. 18, 2010, the Automated Election System Watch (AES Watch) is now composed of more than 40 organizations, among them, the University of the Philippines Alumni Association (UPAA), National Secretariat for Social Action-CBCP, Center for People Empowerment in Governance (CenPEG), Philippine Computer Society (PCS) Foundation, TransparentElections.org, Computer Professionals Union, Caucus of DLSU-CCS, NAMFREL, Association of Major Religious Superiors of the Philippines (AMRSP), National Union of Students of the Philippines (NUSP), Philippine Computer Society Foundation; Transparency International-Philippines, National Council of Churches in the Philippines (NCCP), Faculty of Ateneo de Manila Dept. of Information Communications System, UP Dept. of Computer Science and ITTC, Philippine Computer Emergency Response, Movement for Good Governance, Concerned Citizens Movement, Dilaab-Hearts Foundation, Solidarity Philippines, Association of Schools of Public Administration in the Philippines (ASPAP), Sisters Association in Mindanao (SAMIN), Computing Society of the Philippines (CSP), Pagbabago (Movement for Social Change), Alyansa Agrikultura, Ecumenical Bishops Forum, Biliran Kawsa, Workers' Election (WE) Watch, Health Alliance for Democracy, and others. Its President Emeritus is former Vice President Teofisto Guingona, Jr. while its first spokesperson was Alfred Pascual, now UP President.

For information, please contact: Acting Secretariat Office, 304 CSWCD Bldg., Magsaysay Avenue, UP Diliman 1101 Quezon City; TelFax +9299526; email address: aeswatch2012@gmail.com