POST-ELECTION REPORT OF AES WATCH

Recap and Validation of the STAR Card Assessment of the Preparations for the 2010 Automated Elections

October 2010

Table of Contents

POST-ELECTION REPORT OF AES WATCH

Recap and Validation of the STAR Card Assessment of the Preparations for the 2010 Automated Elections

October 2010

I. INTRODUCTION

A. Advocacy of AES Watch

The Automated Election System Watch or AES Watch[1] is a voluntary, independent, and nonpartisan coalition of concerned citizens' groups and individual advocates whose shared concern is the holding of transparent and credible elections. Represented in the coalition are religious, academic, professional, and civil society organizations, among others.[2] In the run-up to the 10 May 2010 elections, AES Watch worked as an informal network in monitoring Comelec's preparations for the first-ever nationwide poll automation in the Philippines. The focus was on concerns related to the readiness and trustworthiness of the automated election system (AES) being set up by Comelec and its technology contractor. The main instrument used for monitoring was the STAR Card or the System Transparency, Accountability and Readiness Scorecard, which listed twenty items of concern. While respecting a unified stand on common concerns under AES Watch, the conveners and partners of the coalition continued pursuing their own respective mandates and advocacies vis-à-vis the elections.

AES Watch had its beginnings in October 2009 when some individuals and organizations found themselves bound by a common cause as signatories to a joint appeal to Comelec for the release of the AES source code for independent review by interested groups as provided by law. With Comelec remaining unresponsive to the appeal, the initial conveners of AES Watch agreed to work together and engage in activities aimed at the broader cause of increasing critical awareness of the AES among the public and media. They saw the need to bring together information technology (IT) experts and election watchdogs that were doing critical studies on the preparations for the AES. The objective was to help ensure the proper and successful implementation of poll automation as envisaged in Republic Act No. 9369 (the "AES Law"). The AES Watch conveners believed that automation was a tool for effecting electoral reform through the use of IT. It must therefore be utilized to enhance the credibility and trustworthiness of elections, while safeguarding voters' rights and the integrity of the vote.

With its STAR Card as the framework, AES Watch pursued a critical and constructive engagement of election stakeholders. It actively engaged Comelec through the series of hearings of the Joint Congressional Oversight Committee (JCOC) on the AES, as well as in various forums, with large or small audiences, with or without media coverage. AES Watch had also consistently communicated its position on emerging issues through letters to Comelec, press releases, and public statements.

Because of the STAR Card's comprehensive yet straight to the point approach, it was able to gain appeal with the different groups that wanted to monitor the Comelec's work on the automated elections but did not know where or how to start. Several groups adopted the STAR Card approach, albeit modified in a way that would highlight their respective organizations' main concerns and advocacies. Soon AES Watch was sought after not only for the STAR Card but for coalition's insights and opinions on various election-related issues.

As the elections neared, AES Watch decided to extend its mandate to the monitoring of the conduct of elections. With technical backing from Eastern Communications, it set up a web-based Citizens' Election Monitoring (CEM) system, which was designed to receive reports from affiliates and volunteers on election problems and incidents, particularly those related to the AES. The CEM utilized the open-source Ushahidi crowdsourcing software. For purposes of sharing information, the operation of the CEM was coordinated with the AES Watch conveners and partners that had also set up similar Election Monitoring systems, such the Center for People Empowerment in Governance (CenPEG) through its Project 3030, the Computer Professionals' Union through its VoteReportPH, and others. Over 1,000 verified incident reports were collected from across the country. These represented a good sampling of election-related problems experienced on and around election day. But given the limitations in the geographic coverage achieved by even the combined Election Monitoring systems of the different volunteer groups, it was likely many more problems were not captured in the incident reports.

B. Description of the STAR Card

The flagship advocacy of AES Watch was the STAR Card. It was devised to serve as a framework for objectively monitoring the progress of Comelec and its contractor (Smartmatic-TIM) in preparing the PCOS-based AES. Under the STAR Card, the AES was assessed for adherence to certain key management and technical requirements which AES Watch considered crucial in making the system credible and reliable. These requirements were based mainly on the AES Law and the Comelec's Terms of Reference and Request for Proposal for the provision of an automated election system (TOR/RFP). They were also grounded on established standards and best practices for system implementation.

The STAR Card listed 20 items of concern that were grouped into four categories: (1) System Setup, (2) Internal Security, (3) Personnel Training and Voters' Education, and (4) Contingency Planning. Each item was rated using a four-point scale: (1) Pass [requirement met], (2) Warning [requirement not yet met but ample time left to remedy], (3) Danger [requirement not yet met and very little time left to remedy], and (4) Fail [requirement not met at all]. The STAR Card assessment of the preparations for the automated elections was done periodically during the four months preceding the elections.

The concerns included by AES Watch in the STAR Card were initially presented at the 17 December 2009 hearing of the JCOC on the AES. Finding merit in these concerns, the JCOC asked Comelec to respond to them.[3] The first assessment of the AES based on the STAR Card was presented to the public in a press conference following the formal launching of AES Watch

on 18 January 2010 at Club Filipino, San Juan. In this assessment, the AES preparations were found to be in the "Danger" zone overall. By mid-April 2010, when the STAR Card assessment was concluded, the ratings showed that the poll automation preparedness was still in danger. System implementation was seen to be at risk given the delays that had compromised to varying degrees the system setup, personnel training and voters' education, and contingency planning. Also, system trustworthiness was put into question as needed internal and other safeguards had been disregarded.

C. Purpose of the Report

This report recaps the final STAR Card assessment of the AES preparations as of mid-April 2010 and evaluates the validity of the concerns raised in the STAR Card against the actual experience in implementing the AES. Through this report, AES Watch hopes to contribute to the appraisal of the May 2010 automated elections being done by citizens' groups and concerned individuals. AES Watch supports such an independent appraisal based on available information to help provide the basis for policy recommendations and law amendments needed to improve poll automation in the Philippines. Among the sources of information are the incident reports received from the different parts of the country through the Election Monitoring systems of various groups. The Election Monitoring reports referred to below in this report are based on a summary prepared by CenPEG of the incidents reported to its Project 3030 monitoring site.

While Comelec and several others have declared the poll automation a success based on speedy results that matched pre-election surveys and exit polls at the national level, lingering doubts abound. Glitches, errors, and deficiencies experienced throughout the country during elections and the subsequent canvassing of votes have made AES Watch ill at ease with the initial claims of success in AES implementation. The big question is: Did the automated election system really operate properly, securely, and accurately as envisaged in the AES Law?

II. MAIN FINDINGS

A. STAR Card Final Ratings

The STAR Card pre-poll assessment of the AES preparations was concluded in mid-April 2010, about three weeks to election day. As of that time, the final ratings of the 20 items of concern in the STAR Card were as follows:

a. System Setup (Will the AES be ready for full implementation by May 10, 2010?)

1. Timely Delivery of Machines – Qualified Pass
2. Quality of Machines – Danger
3. Technology Certification – Fail
4. Availability of Transmission Facilities – Danger
5. Deployment of Machines – Warning
6. Physical Security of Machines – Danger

7. Precinct Specific Ballots – Printing-Qualified Pass; Deployment-Warning
8. Resource Inventory at Voting Centers – Danger
9. Adequate General Instructions – Qualified Pass

b. Internal Security (Will the AES have the necessary safeguards to prevent fraud?)

10. Source Code – Fail
11. Verifiability of Voting and Results – At voting-Fail; At canvassing-Danger
12. Secured Transmission of Results – Fail
13. Initialization of Machines – Warning
14. Random Manual Audit of Vote Counts – Danger

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

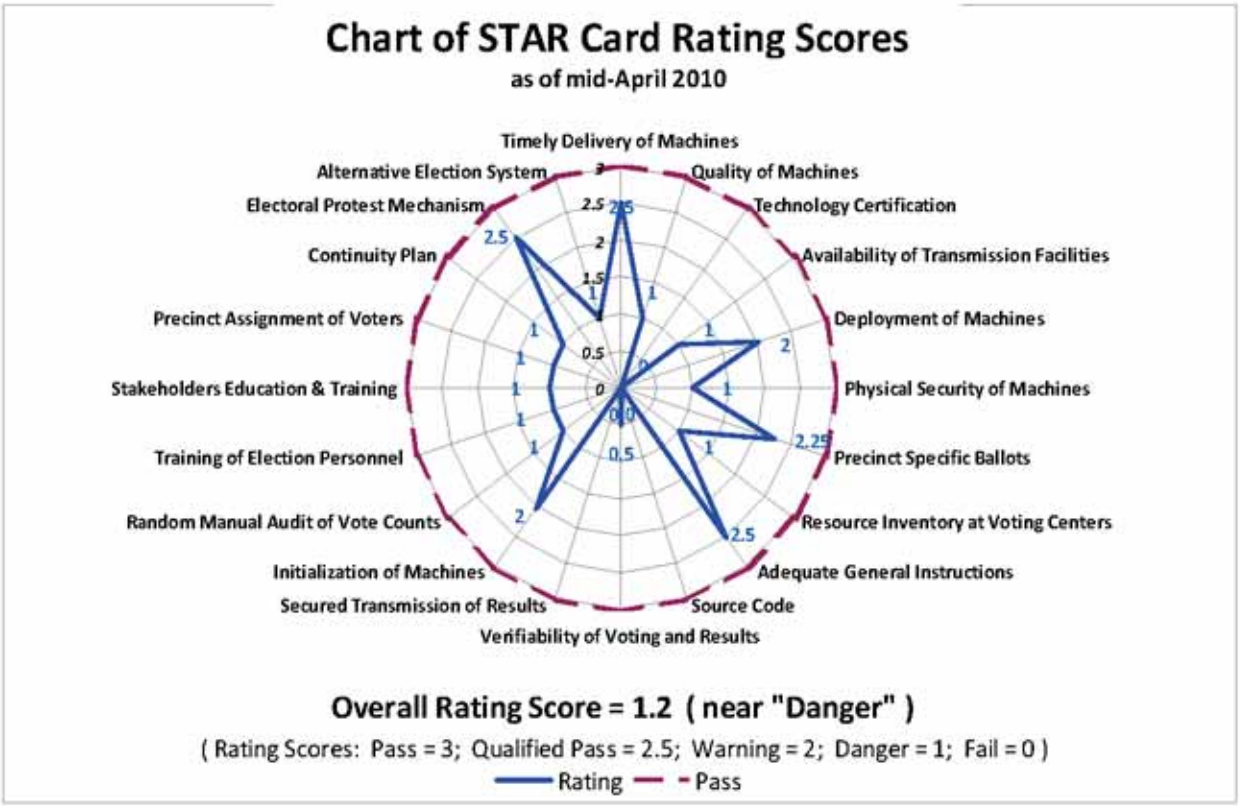
15. Training of Election Personnel – Danger
16. Stakeholders Education & Training – Danger
17. Precinct Assignment of Voters – Danger

d. Contingency Planning (Will Comelec personnel and all concerned know what to do when things go wrong?)

18. Continuity Plan – Danger
19. Electoral Protest Mechanism – Qualified Pass
20. Alternative Election System – Danger

In the foregoing ratings, "Qualified Pass" means that the item so rated was completed but there were qualitative issues associated with its implementation.

Using a scoring system (Pass = 3; Qualified Pass = 2.5; Warning = 2; Danger = 1; Fail = 0), the STAR Card rating would look like the graph illustrated below. In the chart, a clean pass for all the 20 items would have brought the rating to the full circle represented by the broken red lines. But the state of preparedness of the AES as of mid-April 2010 was very much short of the perfect score.



B. STAR Card Assessment of the AES Preparations

a. System Setup

The setting up of the AES by Comelec and its contractor was characterized by (1) delays in the delivery of the PCOS machines with likely compression of time for proper quality testing and configuration, (2) uncertainties in the adequacy of transmission facilities for election results in several voting centers, (3) concerns about the deployment and physical security of the machines (including the CF cards), and, most critically, (4) inadequacies in the technical certification of the AES.

1. Timely Delivery of AES Components

Timely delivery of the PCOS machines and other components of the AES was crucial to the setting up of the AES. AES Watch was concerned that there might not be sufficient time for the long and tedious process of acceptance, configuration, testing, and certification of the machines. Compressed time for the testing of the machines could pose serious consequences on quality assurance.

Change in the AES calendar for at least six times aggravated the concern. The original commitment of the supplier was to complete the delivery of some 82,200 PCOS machines

before 30 December 2009. The actual performance was that only 7,200 units were delivered by that deadline and delivery was completed only in late February 2010. Given the implications for quality of the delayed completion of delivery, this item was rated "Qualified Pass".

2. Quality of Machines

Good quality machines were needed to ensure proper operation of the AES. The lack of reports on the testing and acceptance of machines as they were being received at the Cabuyao, Laguna warehouse of the contractor was a source of concern for AES Watch. In the AES field test held on 20 January 2010, the PCOS machine in one location (Aguho Elementary School) read only 40% of the test ballots. In the mock election held on 6 February 2010, problems with the PCOS machines were experienced in different places: ballot feed problem due to tape on scanner in Ricardo Papa Elementary School; ballot feed jamming twice in Maharlika Elementary School; and 5 ballots rejected with no clear reason for all in New Era Elementary School. These problems indicated deficiencies in the quality testing of the machines before acceptance.

In view of the fact that in no instance had the PCOS machine performance been flawless during the setup period, whether in the field tests or the mock election, the concern about quality of the machines was given a "Danger" rating.

On election day, earlier lapses in quality assurance became evident. Several precincts experienced malfunctioning of the PCOS machines in the form of paper jam, premature shutdown, defective battery, overheating, etc. There were also reports of ballots being trimmed to fit the PCOS machines in certain precincts. According to Comelec, the 465 PCOS machines that malfunctioned represented a small number (0.6 % of total). Smartmatic-TIM had set a threshold of 2.5 % for malfunctioning PCOS machines. Still the problem PCOS machines caused delays in the voting process. In some canvassing centers, the Consolidation and Canvassing System (CCS) computers failed to print the Statement of Votes.

Another evidence of quality assurance failure was the deployment of PCOS machines with erroneously configured CF cards. This oversight, if indeed it was just that, caused tremendous anxiety among the Filipino people. The CF card fiasco is further discussed in item 3 below in connection with technology certification.

Yet another sign of poor quality assurance was the unsynchronized date and time settings of the PCOS machines which, as claimed by Comelec, caused the discrepancies in the date and time stamp on the Election Returns. At the hearings of the Committee on Suffrage and Electoral Reforms of the House of Representatives (HR-CSER), audit logs of certain PCOS machines were presented showing voting outside voting hours, none during voting hours, elections held before or after May 10, etc.

3. Technology Certification

RA 9369 has specific provisions that were designed to give the Filipino voters adequate assurances of the readiness as well as trustworthiness of the AES. Under Section 9 (10) of RA

9369, Comelec is mandated to "establish an independent technical evaluation committee whose main function is to "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 exercise, 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:

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, functionality and security controls of the AES software;
3. The successful completion of a source code review;
4. A certification that the source code is kept in escrow with the Bangko Sentral ng Pilipinas;
5. A certification that the source code reviewed is one and the same as that used by the equipment; and
6. The development, provisioning, and operationalization of a continuity plan to cover risks to the AES at all points in the process such that a failure of elections, whether at voting, counting or consolidation, may be avoided."

By the 10 February 2010 deadline (three months before election day as provided by law), the Technical Evaluation Committee (TEC) failed to issue the certification required by law. In a resolution passed on that day, the TEC claimed successful compliance with just 3 of the 6 requirements for certification: field testing and mock election (item 1), source code review[4] (item 3), and source code kept in escrow with BSP (item 4). In the same resolution TEC stated that the remaining three items were yet to be successfully completed:

1. The successful completion of audit on the accuracy, functionality and security controls of the AES software, which shall be based on the following tests: (a) systems integration test, (b) reliability and accuracy test, (c) security test, (d) volume test, (e) stress test, and (f) electronic transmission/communication test;
2. A certification that the source code reviewed is one and the same as that used by the equipment, which shall only be fully addressed upon completion of the production and configuration of the PCOS and CCS machines in April 2010; and
3. The development, provisioning, and operationalization of a continuity plan to cover risks to the AES at all points in the process such that a failure of elections, whether at voting, counting or consolidation, may be avoided; which in its current draft still needs to be finalized and operationalized through a Comelec en banc Resolution.

Based on the foregoing TEC resolution, the earliest a certification could be issued was April 2010 when the production and configuration of the PCOS and CCS machines would be completed and it could be certified, as specified in the second item above, that the source code reviewed was one and the same as that used by the equipment. However, on 9 March 2010, TEC issued another resolution in which it resolved "to certify, in accordance with RA 9369, that

"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 2010 National and Local Elections." This delayed certification[5] by TEC failed to meet the technical requirements of the law. It was not categorical. It was essentially an expression of a possibility or expectation, it being:

1. premised on certain proposed or future actions still to be implemented (e.g., full adoption of the recommended compensating controls[6]); and
2. partly based on expectations rather than facts as in the case of the required certification "that the source code reviewed is one and the same as that used by the equipment".

Neither was the certification comprehensive. The certification excluded important components of the AES, such as 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 testing.

It should be noted that the field tests and mock election were key requirements in the certification process; they were not exercises intended "shake down the entire system so as to make sure that everything that can go wrong goes wrong now so that we can fix it" (as claimed by Comelec). Successful demonstration of full functionality was critical. The problems encountered in the field tests and mock elections certainly did not demonstrate that the AES was fully functional. Moreover, there was no definite certification that the source code reviewed by SysTest Labs was one and the same as that used by in the machines,[7] and that the components excluded from the certification were fully functional and resistant to fraud, as required by law.

In the assessment by AES Watch, the TEC certification failed to meet the legislated deadline and, more significantly, failed to meet the substantive requirement of the AES Law for a categorical and comprehensive certification. This item of concern was thus given a "Fail" rating.

The faulty compliance with the certification requirement of RA 9369 became manifest, for one, in the massive failure of the PCOS machines to read the test ballots properly during the Final Testing and Sealing (FTS) just barely a week before election day. This was a major glitch in the AES implementation which created an atmosphere of uncertainty in the holding of automated elections by 10 May. Comelec claimed that the problem was due to an oversight in the Compact Flash (CF) card configuration, which, according to Comelec, should have been modified to take into account a late change in the ballot layout. If indeed an oversight, the failure to update the CF card configuration was a clear indication of incompetence. But there were also speculations that the failure was by design, i.e., to have an excuse for gaining access to the CF cards, a vulnerable component of the PCOS machine for cheating purposes. The CF cards served as the memory device for holding ballot images and vote counts. The security of the CF card (against theft, switching, etc.) was part of the STAR Card concern discussed in item 6 (Physical Security of Machines) below.

Over 76,000 pieces of presumably defective CF cards were supposed to have been recalled and replaced prior to elections, but there was never a confirmation of the extent to which this was successfully achieved. Interestingly, Comelec Resolution No. 8905 in the Matter of the Issues that Might Arise During the Final Testing and Sealing and on election day, which specified who had the authority to authorize, among others, the replacement of defective CF cards, was promulgated on 11 May 2010, a day after elections.

Certain post-election findings might also point to the same flawed TEC certification. For instance, the hash code extracted from certain PCOS machines found in a house in Antipolo after elections and subjected to examination by a Forensics Team constituted by the Joint Congressional Canvassing Committee, was not the same as the one published in Comelec's website.[8] The hash code of the software in the PCOS machine was supposed to give an assurance that the software reviewed by SysTest Labs and stored in escrow at the Bangko Sentral ng Pilipinas was the same as that installed in each of the over 82,000 PCOS machines.

4. Availability of Transmission Facilities

The successful operation of the AES would depend on the system's ability to electronically transmit election results from all the clustered precincts. Thus the availability of transmission facilities was crucial. The site survey conducted by Smartmatic-TIM showed (when it was 93% done) that 64% of country had existing connectivity and 32% none. For areas that did not have connectivity, Smartmatic-TIM was making available portable communication devices (5,500 BGAN terminals and 650 VSATs). There were concerns that these numbers might not suffice given that there were over 10,000 voting centers with no connectivity. The concerns were exacerbated by the transmission problems experienced during the field tests and the mock election, even in urban locations. The concern about availability of transmission facilities was given a "Danger" rating.

On election day, transmission problems were encountered as anticipated. Based on the Election Monitoring reports, there were 27 incidents reported involving transmission signal problems which resulted in delays or failures in the transmission of precinct-level Election Returns to the municipal canvassing. These represented about 8% of the number of reported incidents related to problems in the voting centers. In Ilocos Sur, for example, because a number of precincts were unable to transmit the results, the BEIs decided to hand deliver the CF cards together with the PCOS machines to the municipal canvassing center of Sinait, San Juan and Cabugao. This was done in the morning of 11 May 2010, a day after the elections. The same happened in Negros Oriental State University in the province of Negros Oriental. After declaring a failure of transmission, Election Returns (ERs) were manually transported to the canvassing centers. The report pointed out that there was no security escort during the delivery.

At the municipal, provincial and national canvassing levels, 37%, of the reports submitted pointed to significant delays in the transmission of ERs from the precincts. In Pasay City, it was reported that only 302 out of 370 clustered precincts were able to successfully transmit their

results as of 4:30 AM of 11 May 2010. In Kiangan, Ifugao, out of 19 precincts, only 3 had transmitted their ERs to the municipal canvassing center as of 8:00 AM of 11 May 2010. In Iloilo City, only 76 out of 344 precincts were able to successfully transmit the results electronically.

Among the reasons for the delayed transmission of certificates of canvass (COCs) from the municipal and provincial canvassing centers, aside from weak or absence of signal, was the late transmission of results from the precinct level. In Nueva Ecija, on 13 May 2010 or three days after election day, only eight towns and one city had successfully transmitted their COCs to the provincial canvassing center.

5. Deployment of PCOS Machines

AES Watch was concerned about the deployment of the PCOS machines mainly because of the logistical challenge posed by the fact that these machines were precinct specific. Errors in delivery could upset AES implementation. All the PCOS machines were to be picked up from Smartmatic-TIM's warehouse in Cabuyao, Laguna, while the ballot boxes were to be taken from the PhilPost compound in Manila. From these two main warehouses, the contracted logistics companies were to deliver the machines and ballot boxes to their regional or provincial hubs. The machines were to be brought to the precincts before the Final Testing and Sealing process, three to seven days before election day.

Three provincial logistics companies were contracted to deploy the machines and ballot boxes, without going through proper evaluation by Comelec's Special Bids and Awards Committee. The three companies were Germalin Enterprises, Inc.; Argo International Forwarders, Inc.; and Ace Logistics, Inc. No disclosure was made on their capabilities as logistics providers. According to its latest documentations (2006) in the Securities and Exchange Commission (SEC), Germalin, which was to deliver the machines in the National Capital Region, had gross revenues of P63 million. Ace, which would cover the rest of Luzon, had a reported income of P18 million in 2008, but its properties and equipment were reported to be only P1.77 million. Argo, which would take care of deliveries in Visayas and Mindanao, generated P2.4 million profits in 2001, but lost P1.4 million in 2002.[9] Among the three logistics companies, only Germalin was reported to have its own trucks for delivery of the machines. Ace and Argo, which were tasked to cover larger areas, would reportedly rely on subcontractors from the localities to help in the delivery of the machines. Both Germalin and Argo had had precious contracts with Comelec in past elections for delivering election paraphernalia. Argo was the forwarding company contracted by Smartmatic to deliver its voting machines during the 2008 ARMM elections.

Due to the limited disclosure of information about the capabilities of the three logistics companies contracted by Comelec, the concern about deployment of machines was given a "Warning" rating as of mid-April 2010.

Actual delays in deliveries of PCOS machines and ballot boxes were reported from different areas around the country to the Election Monitoring systems of volunteer groups. Some of the deliveries were so delayed that the machines arrived only the following day (after 10 May), as

reported in Kauswagan, Lanao del Norte. In Maasin City, Southern Leyte, on the other hand, delivery setbacks were caused by the absence of a secure area for the storage of the machines. The scheduled delivery of 20 of the total 89 expected PCOS machines were affected. Based on the Election Monitoring reports, there were six incidents of late arrival and two incidents of accident during delivery.

6. Physical Security of Machines

The machines, including the CF cards, should be securely protected from theft or tampering in their assigned locations to ensure the holding of clean and honest elections. The CF card, which would record of votes, was supposed to be sealed in the PCOS machine but could be removed and replaced in case of PCOS malfunction. CF cards should thus be protected from snatching, switching, and other risks. The political parties were supposed to be free to send their poll watchers to secure the machines themselves but there was no clear agreement yet as to how security was going to be done as of mid-April 2010 and time was running out. The concern about physical security of the machines was given "Danger" rating.

The Election Monitoring reports indicated 5 incidents of security problem during PCOS/ ballot box delivery or in the storage area. Also reported were two PCOS machines that were deliberately destroyed in the Mountain Province: one was hammered and the other burned after poll closing. Further, 60 PCOS machines were discovered after election day in a house in Antipolo City and brought to the Senate for safekeeping. This clearly indicated a breach in the physical security of the machines. The Smartmatic technician who was found in possession of the machines reportedly decided to bring them home when no one collected them from certain voting centers (unclear from which and how many voting centers) and the City Treasurer of Antipolo refused to accept them. Still, how the Antipolo PCOS machines went astray and how they were used during the elections have not been fully established.

7. Precinct-Specific Ballots

The concern of AES Watch with regard to the precinct-specific ballots was related to timely and error-free printing and delivery. Will the ballots with pre-printed names of candidates for specific localities be ready in time? There were more than 1,600 types of ballot faces to be printed and delays were being experienced due partly to printing capacity problems and partly to delays in the finalization of the list of qualified candidates. The scheduled commencement of ballot printing for 25 January 2010 was postponed for a week.

Ballot delivery was contracted to Air21, which is one of the largest logistics companies in the country. Air21 started the nationwide distribution of ballots on 25 April 2010, two weeks before elections. The official ballots were picked up from the National Printing Office compound, the government agency contracted to print the ballots. These were delivered directly to the Municipal Treasurer's Office, where they were inspected by the Board of Election Inspectors (BEIs) and kept for storage. The ballots were later taken by the BEIs on election day to be brought to the voting centers.

As of mid-April 2010, the printing of ballots was completed although there were issues such as that related to the authenticating mark to be read under ultraviolet light. Thus the printing aspect was rated "Qualified Pass" and the concern with ballot deployment was given a "Warning" rating.

From the Election Monitoring reports, there was one incident of error in ballot delivery, one incident of late arrival, and one incident of non-delivery. From other sources, it was learned that ballots destined for Caloocan were wrongly delivered to Malabon. This led to a one-hour delay in start of voting. There was also the case of ballots destined for precincts in Brgy. Buenos Aires, Pagsanghan town in Samar were wrongly brought to Brgy. Generosa, Guimbal, Iloilo. A failure of elections was declared in both areas, and special elections were held on 3 June 2010.

8. Resource Inventory at Voting Centers

The voting centers needed various resources to ensure the successful operation of the AES. Among these were IT-capable personnel for the BEIs, working transmission facilities, reliable power supply, etc. By mid-April, the concerns were mainly related to the availability of IT-capable personnel (see item 15 below) and transmission facilities (see item 4 above) which were given "Danger" ratings.

9. Adequate General Instructions

General Instructions (GIs) were needed to guide the BEIs and the Board of Canvassers (BOCs) on the conduct of the AES. The initial concerns of AES Watch about the GIs were related to the delay in their issuance and the inadequacy of their coverage. Comelec issued initially Resolution No. 8739 dated 29 December 2009 on GIs for the BEIs on the Voting, Counting, and Transmission of Results. A revised version was subsequently issued under Resolution No. 8786 dated 4 March 2010. Among the revisions were a new section on the procedure in case of a shortage of ballots and an improvement of the provision on the handling of ballots rejected by the PCOS machine. At the same time, a revised provision that removed digital signing in the transmission of election results became a major concern (see discussion on secured transmission of results in item 12 below).

The GIs for the BOC on Consolidation, Transmission, and Canvassing of Votes were finalized on 30 March 2010 with the issuance of Resolution No. 8809.

As of mid-April 2010, requirement for GIs was considered "Qualified Pass" under the STAR Card.

b. Internal Security

The main issues regarding the internal security and trustworthiness of the AES were: (1) lack of independent source code review by interested groups and political parties, (2) absence of voter verification to show that the PCOS machine registered the voter's choice, and (3)

disabling of the digital signature function in the system. The random manual audit was supposed to serve as a "fallback" safeguard for validating the accuracy of the vote count by the PCOS machine. However, the long delay in the release of the audit results has diluted its value.

10. Source Code Review

Section 12 (14) of RA 9369 mandates, "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." The source code review provided for in this section of the AES Law should be distinguished from the source code review required under Section 9 (11). The latter was to be performed by an international certification entity to meet one of the requirements for the TEC certification (see item 3 above). The source code review under Section 12 (14) was evidently for the purpose of giving political parties and other election stakeholders the opportunity to do an independent review of the source code.

The provision of the AES Law on open source code review was reflected in the Comelec TOR/RFP, specifically in Section V (Other Specifications No. 7.4), which says, "The winning bidder shall authorize Comelec to make the final source code of the PCOS & CCS and all of its components available and open to any interested party or groups which may conduct their own code review thereof." Interestingly, however, the source code review by interested political parties or groups was not included in Comelec calendar for AES preparations.

The source code is a human-readable version of the computer programs running on the different hardware components of the AES, namely, the Election Management System (EMS) machines, the Precinct Count Optical Scan (PCOS) machines, and the Consolidation and Canvassing System (CCS) machines. Reviewing the source code can reveal whether the programs will do the functions required of the machines correctly and accurately, whether the programs are free of malicious codes or instructions, and whether the programs conform to the requirements of the AES Law and the Comelec TOR/RFP for supply of the AES.

On 26 May 2009, soon after the selection of Smartmatic-TIM as supplier of the AES technology, the CenPEG, a convener of AES Watch, submitted to Comelec a letter of interest to review the source code of the selected technology. In the same letter, CenPEG requested for a copy of the source code pursuant to Section 12 (14) of RA 9369. On 10 June 2009, Comelec *en banc* approved the release of the source code through its Minute Resolution No. 09-0366 but the approval was delivered to CenPEG only on 10 July 2009, the day of the contract signing between Comelec and Smartmatic-TIM. In response to a follow-up from CenPEG, Comelec explained that the source code they had then was not yet the source code for implementation, that it was a baseline source code that had yet to be customized, and that it had to be certified first by an international certification entity prior to release for review by interested political parties or groups. Rejecting Comelec's excuse, CenPEG filed a petition for mandamus with the Supreme Court on 5 October 2009, seeking to compel Comelec to immediately make the AES source code available.

In the meantime, with the source code not having been released yet, a group of concerned individuals and organizations, some of which eventually became the nucleus of AES Watch, got together and agreed to present to Comelec a Joint Appeal for the Release of the Source Code. The appeal was delivered on 5 October 2009 backed by over 200 signatories. No response was received from Comelec.

In an attempt to comply with Section 12 (14) of the AES Law, Comelec invited representatives from interested political parties and groups to a meeting on 1 February 2010 to present and discuss the guidelines for the conduct of a so-called source code review. In the said meeting, the attendees expressed concern on the restrictive conditions being imposed by Comelec and the waning period for the review. Nothing was resolved in that meeting. In the meantime, the Liberal Party had tendered its own letter of intent and informed Comelec that it had engaged the services of KPMG to review the source code.

On 19 February 2010, some political parties and groups, including AES Watch, issued a joint statement in which the signatories pointed out that the guidelines issued by Comelec for its so-called source code review were too restrictive and asked that the same freedom and latitude granted to SysTest Labs be given also to political parties and groups interested to do a proper source code review. The joint statement was faxed to Comelec on 20 February 2010 and a printed copy hand delivered to Comelec on 22 February 2010. Comelec did not respond to the joint statement.

Then, on 24 March 2010, with just 47 days to elections, Comelec convened another meeting with interested political parties and groups to re-initialize discussions on the source code review. In the meeting, the attendees were advised that a facility had been prepared by Comelec where interested political parties and groups could access the source code, but that if a reviewer intends to use automated tools for the review, these should be presented to Comelec for approval. When asked if the original guidelines had been amended, Comelec responded in the negative. There and then, the Liberal Party representative confirmed the withdrawal of its letter of intent to participate in the review due to the restrictive conditions and lack of material time. The AES Watch representative echoed a similar position..

AES Watch took the view that the source code review that was being scheduled by Comelec after certification by SysTest Labs in February 2010, with limited time left before election day and under restrictive rules, would just be a mere “walkthrough”. Without a proper review of the source code by interested groups and political parties, the reliability and trustworthiness of the system was put in doubt.

Given Comelec’s failure to provide the conditions needed for a proper source code review by interested groups and political parties, AES Watch gave this item of concern a “Fail” rating.

In the actual operation of the AES, certain computer errors were experienced, which if not the result of deliberate manipulation, were clearly bugs in the system. Among these errors were the miscalculation of the total number of registered voters (156 million instead of just 51 million) and the premature date and time stamps in the audit logs of some PCOS machines. At

the canvassing hearing on 26 May 2010, a Smartmatic official reportedly admitted that this was an error in programming. Also, the aforementioned forensic examination of the so-called Antipolo PCOS machines revealed that through the Console Port present in the PCOS machines, the program running the machines could be accessed and controlled by connecting another computer. It was found that the access could be achieved without having to enter a username-password combination and that the log was saved to a volatile memory, which is lost every time the machine is turned off leaving no detectable trace of any the intrusion.

The position taken by AES Watch on the obligation of Comelec to release the AES source code for review under Section 12 (14) of RA 9369 was vindicated when, on 21 September 2010, the Supreme Court granted the petition for mandamus filed by CenPEG on 5 October 2009, directing Comelec to make the source codes for the AES available to CenPEG and other interested parties or groups for independent review.

11. Verifiability of Voting and Results

Section 7 (6) of RA 9369 provides for the minimum functional capabilities of the AES. One of these is the requirement to "provide the voter a system of verification to find out whether or not the machine has registered his choice." The voter verification function was available in the PCOS machines but was disabled by Comelec, presumably to save on voting time and speed up the voting cycle. Without such vote verification process, however, there would be issues of transparency and credibility in the reading of ballots and counting of votes. The voters would never know if the PCOS machine had registered their choice correctly. Voters' rights would thus be compromised.

The AES Law has provisions that apply only to national positions (president, vice-president, and senators) for verifying the authenticity of the certificate of canvass against Election Returns of precincts. The law is silent about rules regarding authenticity of canvassing at the provincial, city, district, and municipal levels. As a remedial measure, there were suggestions for Comelec to install LCD projectors at the canvassing centers to show on a large screen the equivalent of the statements of votes (SOVs) so that political watchers and citizens' arm watchers could easily verify the contents of the SOVs using the printed copies they hold of the Election Returns as obtained from the clustered precincts. This arrangement was intended to promote transparency at the canvassing centers.

Comelec did eventually recognize the need to facilitate the widest coverage and bolster the transparency of the canvassing of election results and thus issued Resolution No. 8825 on 23 April 2010, "requesting the Local Government Units (LGUs), through the Department of Interior and Local Government (DILG), to provide/make provisions for LCD projectors for each of the Municipal/City/Provincial/District BOCs within their respective territorial jurisdiction, to display/project the contents of the CCS laptop screen during the canvassing of election results…"

In view of the disabling of the function voters could use to verify whether or not the PCOS machine had registered their choice, AES Watch gave a "Fail" rating to the verifiability of votes

at the clustered precincts. At the local canvassing centers, a "Danger" rating was given as of mid-April to the verifiability of results due to the lack of clarity at that time as to how Comelec would provide the transparency needed in the canvassing of election results.

As noted above, Comelec did make an attempt to facilitate verification of votes being canvassed at the local canvassing centers when it issued Resolution No. 8825 on 23 April 2010 requesting LGUs to provide LCD projectors. Given that the installation of such projectors was not mandatory, it was not clear to what extent LGUs obliged Comelec. Furthermore, some incident reports indicated that actual use of LCD projects was uneven. In Pasay, for instance, the LCDs reportedly displayed only the status of transmissions from the precincts. When asked if the Election Returns received could be displayed, the Pasay BOC replied in the negative.

12. Secured Transmission of Results

Section 19 (22) of RA 9369 provides, "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." Based on this provision, the key to secured transmission was the digital signature. However, it was not clear if and how the digital signing would be done.

The revised GIs for the BEI issued on 4 March 2010 changed the procedure for transmission of results from the PCOS machines by instructing the BEI not to digitally sign the transmission. This was in contravention of the requirement of the law. Without the mandated digital signature on the electronically transmitted election results, data manipulation could be effected. Comelec explained that the digital signature would remain to be existent through the use of the iButton by the BEI Chairman and two passwords by the two other BEI members upon opening of the PCOS machine immediately before counting, printing and transmission. Assuming the iButton would actually trigger the digital signing, still it was the vendor who generated the assigned signing keys and therefore if the opportunity would arise and if there was motive, any one who had access to the keys could manipulate the election results and their transmission.

SysTest Labs' Certification Test Report Summary dated 8 March 2010 found in its transmission test that "...the digital signature could not be verified..." A manual compensating control it recommended in this regard was: "To validate the accuracy of the automated count, a relevant statistical sample of manual vote counts in key polling locations should be performed. This should be followed up with a tracing of the count moving up the reporting hierarchy to further validate the reporting chain as being intact." No procedures were formulated for either Comelec or PPCRV[10] to implement the SysTest Labs' recommended "tracing of the count moving up the reporting hierarchy".

AES Watch found that there was no convincing explanation as to how secured transmission of election results could be achieved. What was evident was the explicit instruction to the BEI not to digitally sign the transmitted results. Thus this item of concern was given a "Fail" rating.

Post-election developments have indicated that the digital signature implemented for the AES was not sound technically or simply absent. In the hearing conducted by the HR-CSER, it was revealed that what was implemented was a "machine digital signature", something that is not legally recognized. Further, the Forensic Team constituted by the Joint Congressional Canvassing Committee found in the PCOS audit log an entry stating "No BEI key with which to sign results" indicating that there was no digital signature affixed to the election return. Also, during the forensic examination of certain PCOS machines, the Smartmatic technician could not demonstrate how the digital certificate can be extracted or displayed saying that they did not have the necessary (software) tool to do so.

A weakness of the AES that surfaced in the canvassing of electronically-transmitted vote counts was its inability to distinguish between the Election Returns generated during the Final Testing and Sealing (FTS) of the PCOS machines and the legitimate Election Returns generated on election day itself. The CCS machines and the Comelec central and backup servers failed to block the FTS results transmitted from some PCOS machines. If transmission was secure, then only legitimate election results (i.e., counts of votes made on election day) should have gone through the electronic reporting chain.

Post-election examination of AES machines showed incredible or anomalous date and time stamps. At the hearings of the HR-CSER, for instance, audit logs of certain PCOS machines were presented showing transmissions at improbably late hours or even days after. These findings have raised questions on the authenticity and integrity of the transmitted election results. Were the discrepancies due to a faulty audit mechanism of the AES or due to an outright fraud that the system was not able to block? How secured were the transmissions after all?

13. Initialization of PCOS Machines

Comelec required that the PCOS machines at the clustered precincts be cleared or "zeroed out" on election day before the start of voting to show that are no pre-stored votes in the PCOS memory (CF card). This requirement was formalized in Comelec Resolution No. 8739 dated 29 December 2009 on GIs for the BEI and its revised version, Resolution No. 8786 dated 4 March 2010. The initialization process was to be concluded with the printing of a report showing zero ("0") vote for each candidate.

AES Watch expressed concern with the possibility of pre-stored votes in the CF card given that the memory capacity of card is much larger than what is needed for storing the images of just actual ballots cast. The initialization procedure seemed inadequate to give assurance that there was no pre-loading of the CF cards with votes that would be treated as or included in the vote count after the voting period.

Furthermore, AES Watch was concerned that the initialization process did not include any procedure to verify the integrity of the programs installed in the PCOS machine (e.g., by performing hash value computation on the machine and comparing the computed value with the hash value from the approved program). It should be recalled that the TEC certification did

not ascertain that "the source code reviewed is one and the same as that used by the equipment." A malicious program running on the machine would make internal rigging of results possible.

In some public forum, a Comelec Commissioner gave a verbal assurance that the concerns of AES Watch regarding the initialization of PCOS machines would be addressed. This item of concern was thus given a "Warning" rating.

Election day came and no improvement in the initialization procedure was introduced. In the post-election forensic examination of the Antipolo PCOS machines, it was found that the hash code extracted from a machine that was examined was not the same as the one published in Comelec's website. The hash code of the software in the PCOS machine was supposed to give an assurance that the software reviewed by SysTest Labs and stored in escrow at the Bangko Sentral ng Pilipinas was the same as that installed in each of the over 76,000 PCOS machines.

14. Random Manual Audit of Vote Counts

Section 24 (29) of RA9369 mandates, "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. Any difference between the automated and manual count will result in the determination of root cause and initiate a manual count for those precincts affected by the computer or procedural error."

In its Minute Resolution No. 09-0765 dated 10 November 2009, Comelec created the Technical Working Group on the Random Manual Audit (TWG-RMA)[11] to recommend procedures for the conduct of the RMA. But for over three months, there were no indications as to which direction the RMA was moving. To AES Watch and other election watchdogs, the safeguard provided by the RMA had become central to ensuring the integrity of the automated elections given that their pleas for measures to address internal vulnerabilities of the AES had remained unanswered. Even SysTest Labs in its Certification Test Report Summary dated 8 March 2010 highlighted as a compensating control the following: "To validate the accuracy of the automated count, a relevant statistical sample of manual vote counts in key polling locations should be performed."

A key issue on which consensus was needed related to the appropriate audit sampling methodology to achieve a comfortable level of confidence in the accuracy of the vote count by the PCOS machines. To discuss the issue, AES Watch convened a small group of statisticians, mathematicians, survey practitioners, and IT professionals in a Roundtable on the Random Manual Audit which was held on 29 March 2010. The group concluded that (1) the provision of the AES Law on the RMA sample size was too low and should be expanded, (2) the precincts to be audited should be known only during the day of the elections (preferably towards the closing time on election day), (3) the RMA should be done before the proclamation of candidates (preferably right after the close of voting), (4) the RMA should be performed by independent auditors, and (5) the actual conduct of the RMA should be open and transparent.

By 30 March 2010, the TWG-RMA finally submitted its recommendations. As approved by Comelec in its Minute Resolution No. 10-0453 dated 5 April 2010, the key recommendations were the following: (1) 5 precincts per legislative district or a total of 1,145 for the 229 districts to be audited, (2) audit to be done after the shut down of the PCOS, (3) random selection of the precincts to be done manually, (4) audit to be done by BEIs from the same or nearby voting center, (5) all national positions and five local positions (representative, governor, vice-governor, mayor, and vice-mayor) to be audited, and (6) no interpretation of the voter's intent to be done in the appreciation of ballots by the auditors. It was not until 30 April 2010 through Resolution 8837 that Comelec en banc promulgated the General Instructions that detailed the conduct of the RMA, including the composition and appointment of the RMA Team, the guidelines on reading the ballots and the effects of discrepancy between AES and RMA counts.

At the time AES Watch concluded its STAR Card evaluation in mid-April 2010, no general instructions on the RMA had yet been issued by Comelec and time was running out. Thus the RMA concern was given a "Danger" rating.

The final report of the TWG-RMA on the results of the random manual audit came out only on 20 July 2010, more than two months after the closing of the 10 May 2010 polls. Only 1,046 sample clustered precincts were audited, about a hundred short of the original target. From the report of TWG-RMA, it was evident that the RMA was not accorded the importance it deserved as a crucial control measure – a test on the accuracy of the automated vote count by the PCOS machines. Preparations were haphazard. According to the report, the RMA "did not have any allocation in the AES supplemental budget, nor in Comelec's agency budget" and "had to rely on the benevolence of various Comelec offices in terms of staff, space, supplies and other such contingencies…" The 3,435 teachers who constituted the RMA Team were selected from those without assignments as BEIs in the 10 May elections. They were given only a one-day session of training one week prior to elections and not all were able to participate. The RMA was thus characterized by significant variances in the reading of votes in the ballot.

The raw findings of the audit were subjected to two rounds of validation (an initial and a final) that reduced large variances. After such validation, the TWG-RMA reported an accuracy rate that ranged from 99.50% to 99.64% across the five positions audited. The average accuracy rate can be placed at 99.6%, which is equivalent to a margin of variance of 0.4% (i.e., 4 out of every 1,000 ballot marks were incorrectly interpreted by the PCOS machines). While well within the minimum of 99% accuracy rate set in Comelec's RMA guidelines, the 99.6% accuracy rate was below the minimum 99.995% accuracy rate imposed on the PCOS machines in the Comelec TOR/RFP (which allows at most 1 variance out of 20,000 ballot marks). In its report, the RMA Team said that the 99.995% accuracy would be difficult to ascertain since the human appreciation of the ballot is different from the way the machine interprets the ballot. But this is precisely what Comelec did when it evaluated the accuracy rating of the PCOS machine, a procedure that should have been maintained as a standard. The Final Testing and Sealing was another case of doing a manual count (which relied on the human appreciation of the ballot) to verify the machine count.

c. Personnel Training and Voters' Education

The May 2010 automated elections involved a new way of voting, counting, and canvassing for the over 300,000 election personnel (BEIs, BOCs, etc.) and about 51 million voters, all requiring adequate training and/or education. In addition, Comelec's technology contractor needed to recruit, train, and deploy 45,000 technicians to fix technical problems at the voting centers. Delays and unclear preparations were a source of major concern. Election personnel training and voters' education were found lacking intensity and substance.

15. Training of Election Personnel

Automated elections being implemented for the first time would rely heavily on adequately trained teachers assigned to the BEIs and BOCs. These personnel should be able to ensure proper operation of the machines and undertake simple troubleshooting when needed. In particular, Section 3 (3) of RA 9369 requires, "at least one member of the Board of Election Inspectors shall be an information technology-capable person, who is trained or certified by the DOST…" Similarly, Section 5 (4) of the same law provides, "each board of canvassers shall be assisted by an information technology-capable person authorized to operate the equipment adopted for the elections."

Comelec Executive Director Jose Tolentino stated at the 17 December 2009 JCOC hearing that the training for teachers to constitute the BEIs would start on 18 March 2010 instead of the original 20 January 2010 schedule called for in the Comelec calendar of 10 October 2009. The shortcutting of time allotted for training and certification alarmed the teachers who were worried that this delay would leave them inadequately trained in operating the machine. Comelec announced later that the training would be advanced to 1 March though as early as 18 January, AES Watch had already raised the "Danger" sign with regard to this concern. To AES Watch and its conveners, the concern regarding the election personnel was "not because of any perceived incompetence, but because of the pitfalls of late instructions given to them".[12]

The initial training sessions of BEI members dealt with the basics of the PCOS machine: its parts and how to operate it. Comelec clarified that these training programs were intended to prepare the members of the BEI for the Final Testing and Sealing. The teachers were told that training for transmission would be done on a separate date, although there was no clear date as to when this would be conducted. Post-election verification, however, revealed that no training on transmission was ever conducted for the BEIs and the BOCs.

Given the tight implementation timelines, questions were also raised as to how Comelec and its AES contractor would be able to recruit, train, and deploy 45,000 competent technicians needed to provide technical support to the BEIs and BOcs on election day. As seen during the elections, many cases of procedural error and machine malfunction could be attributed to the lack of preparedness of the BEIs, BOCs, and even Smartmatic-TIM field personnel to prevent or resolve such problematic situations.

One specific indication of the deficiency in the training of the BEI members was the failure to fully implement the add-on job of manually scanning each ballot with a hand-held ultraviolet (UV) lamp to verify its authenticity.[13] In fact, the General Instructions for BEIs was not amended at all to include the use of the UV lamps. Based post-election reports, only about 50% of the BEIs did the ballot scanning with the UV lamp. While some precincts did not receive any UV lamps, those that had them did not all bother to use them. Some even mistook them for emergency lamps.

Also, the SysTest Labs' Certification Test Report highlighted the need for Comelec to fully adopt appropriate manual processes and/or compensating controls to address the weaknesses it identified in the AES voting system and make the system "capable of operating properly, securely and accurately". There no reports on whether or not training on these controls were given to the BEI and BOC members.

On election day, crowd management turned out to be a major challenge to many BEIs. This aspect of the BEIs responsibility did not seem to have been covered in their training.

16. Stakeholder Education and Training

The AES law mandates that Comelec, as the election manager, and Smartmatic-TIM, as the technology supplier, shall take charge of the voters' education. Section 26 (31) of RA 9369 states that Comelec "shall, not later than six months before the actual automated election exercise, undertake a widespread stakeholder education and training program, through newspaper of general circulation, radio, television and other media forms, as well as through seminars, symposia, forums and other nontraditional means, to educate the public and fully inform the electorate about the AES and inculcate values on honest, peaceful, orderly and informed elections." On the other hand, Component 3 (Overall Project Management) of the Comelec TOR/RFP also included, as part of the services of the technology supplier, training on "change management" as well as voter education and training. The PPCRV, as the lone Comelec-accredited citizens' arm, was also tasked to assist in this enormous task.

The voters' education focused much on shading the "bilog na hugis itlog" and did not involve a holistic approach that should have included sensitizing the voters to the critical vulnerabilities of the AES and the possible impacts of the AES on voters' rights. For instance, AES Watch volunteers who interviewed participants in the mock election held on 6 February 2010 at the New Era Elementary School revealed that they were concerned whether their votes were accurately read by the machine despite making sure that the ovals on the ballot were fully shaded. It was not clear how voters' education conducted by Comelec and PPCRV had addressed this concern.

Comelec had relied mainly on the use of media for voters' education. While it is true that media has the farthest reach and is the highly accessible source of information, it nonetheless lacks "personal touch" and does not give voters a chance to ask questions or try the PCOS machine hands on. Pulse Asia's January 2010 Survey showed that 71% of Filipinos had little or almost no knowledge at all of the AES (79% among socioeconomic class E which accounts for a

many as 30% of the population). If these percentages were to be applied to the 51 million registered voters, there could be as many as 12 million voters in class E who needed to be trained on the AES in a more interactive mode. These low-income voters might not have been within the reach of the media-based training programs provided by Comelec.

Moreover, Comelec officials at the local levels blamed lack of funds coming from the national office for not being able to conduct more extensive public demonstration of PCOS-based voting. Independent volunteer groups that conducted voters' education in far-flung areas found that indeed the voters had so many questions about the new voting system that media failed to address. AES Watch thus rated the concern about voters' education to be in "Danger".

17. Precinct Assignment of Voters

To minimize confusion on election day, voters were advised to check ahead their assigned precinct under the new system of clustering of precincts. The voters list should be posted in public spaces such as the barangay or town hall, parishes and voting centers before 10 May 2010. On Election Day, however, there were still cases of voters failing to locate their names in the list. In a post-election survey conducted by SWS, problems on finding ones' name on the voters' lists became worse this year (6%) compared to the 2007 elections (3%).

One way by which voters could check their clustered precinct assignment was through the online Registration Verification Precinct Finder on Comelec's website. Unfortunately, only those with Internet access could utilize this facility. The concern with precinct assignment of voters was given a "Danger" rating.

d. Contingency Planning

Finalization of the continuity plan was very much delayed. There was no more time to operationalize it. Election personnel were not trained and drilled, if at all, on the contingency measures provided for in the plan.

18. Continuity Plan

Section 11 (13) of RA 9369 provides, "The AES shall be so designed to include a continuity plan in case of a systems breakdown or any such eventuality which shall result in the delay, obstruction or nonperformance of the electoral process". Adoption of an operational continuity plan was also a requirement for the TEC certification as provided for in Section 9 (11) of the same law.[14] The main purpose of the continuity plan was to avoid a failure of election in case of problems with operation of the AES at counting, canvassing or consolidation.

By mid-April 2010, the continuity plan had not yet been finalized. The draft circulating then appeared inadequate and it was not clear if a satisfactory version that incorporated the suggestions from election stakeholders was forthcoming. Hence, the concern with the continuity plan was given a "Danger" rating.

Finally on 30 April 2010, Comelec promulgated Resolution No. 8839 on Contingency Procedures to be Adopted as Supplement to the General Instructions to the BEI and the BOC. These procedures constituted the continuity plan. Included in the plan were the organizational structure for its implementation and the contingency procedures applicable to the national/ central canvass service, the BOCs at the LGU levels, and the PCOS system. While the plan was finalized before election day, there was very little time left for the adequate training on the plan to be provided to the concerned election personnel such as the technology supplier technicians, and the BEI and BOC members. There were no drill exercises to simulate problems, like PCOS auto shutdown, failure to print or transmit, etc. Drill exercises should have been a vital component of any disaster management or continuity plans.

19. Electoral Protest Mechanism

There are no specific legal provisions available for settling AES-based election disputes so there was a need for Comelec to promulgate the applicable rules. Thus the promulgation of an appropriate election protest mechanism became one of the concerns of AES Watch and included in the STAR Card.

It was not until 22 March 2010 that Comelec issued Resolution 8804 which sets the rules of procedure on disputes in an automated election system. The rules apply to election disputes under the PCOS-based AES and cover pre-proclamation controversies and election protests. The item on electoral protest mechanism was rated "Qualified Pass" as of mid-April 2010.

Comelec records show that at least 100 election protests from 41 provinces and cities had been filed by June 2010.

20. Alternative Election System

In the run-up to the May 2010 elections, there was a lot of anxiety about Comelec's ability to achieve timely completion of preparations for the AES. Comelec officials themselves were talking about the possibility of automation failure and going into manual count in up to 30% of the precincts. As a contingency measure, the preparation of an alternative election system was thus included by AES Watch in its STAR Card. Should implementation of the AES in certain localities prove to be impossible, manual counting, transmission, and canvassing would have to be resorted to. Guidelines for the manual conduct of elections and for the interface of this with the AES would have to be promulgated accordingly.

By mid-April 2010, no guidelines had yet been issued, so this concern about having a ready alternative voting system in case of automation failure was given a "Danger" rating.

Comelec did not at all issue any resolution specifically on the procedures for the manual conduct of voting, counting, and canvassing as a contingency measure. Even the continuity procedures contained in Comelec Resolution No. 8839 dated 30 April 2010 did not include any guidelines on such manual operations. The measures in the resolution were so designed as to take care of contingencies within the AES itself, such as, by using the PCOS machine in a nearby

precinct if a precinct's own PCOS machine failed and could not be replaced or by physically transporting the CF card containing the record of votes if electronic transmission failed. Other Comelec resolutions related to the AES, however, do have provisions referring to manual procedures. For example, Rule 5 under Resolution No. 8804 dated 22 March 2010 pertains to the canvass of manually prepared election returns (i.e., "manually prepared by reason of the implementation of a continuity plan").

III. CONCLUSION

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 to the Election Monitoring systems of AES Watch and its partners, 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.

The extent and magnitude of the problems that afflicted the recent elections may not be established simply on the basis of largely anecdotal reports. Still, there is a preponderance of reports that cast doubt on claims that the AES voting system for which the Filipino people spent P11 billion was a "rousing success". The reported problems and incidents indicate otherwise. The question remains: Did the AES operate properly, securely, and accurately?

Comelec has in its possession the pertinent information (e.g., contracts, reports, minutes of meetings, performance and operational data, etc.) needed to shed light on what the AES was intended to do and how it actually operated. This information, which has so far been withheld, must be publicly disclosed in accordance with the constitutional guarantee on freedom of information. With such information, Filipino expert groups could undertake independent, empirical studies to fully evaluate the level of performance achieved by the AES. The results of such studies would not only help clear the air on issues surrounding the AES but also, more importantly, provide a solid basis for planning improvements for poll automation in the country.

Through this report, AES Watch makes an urgent call to Comelec for the release all pertinent information on the AES.

References

Averia Jr., Angel S. (President, PHCERT and IT Consultant, CenPEG). AES: Did the AES Operate Properly, Securely, and Accurately? Center for People Empowerment in Governance (CenPEG). 4 September 2010.

Averia, Jr., Angel S. (President, PHCERT and IT Consultant, CenPEG). The Automated Election System and Information Security. (Presented to the UP College of Law, Quezon City, 2010).

Bahague Jr., Ricardo. VoteReportPH: New tools for old problems (Prometheous Bound). Manila Times, 3 June 2010. (Found in www.VoteReportPH.org)

Calub, Adelina P. Digital Signature / Electronic Signature. MIPOLAW. September 2010.

Casino, Edmundo G. Post-May 10, 2010 National Elections AES Fraud Analysis. Computer Society of the Philippines. 23 September 2010.

Castillo, Nadja Alvarez. Project 3030 Election Monitoring Incident Reports. Center for People Empowerment in Governance (CenPEG). Draft as of 31 August 2010.

Center for People Empowerment in Governance (CenPEG). 30 Vulnerabilities, 30 Safeguards. Quezon City. February 18, 2010. (Published under Project 3030 with the support of the European Union).

Center for People Empowerment in Governance (CenPEG). A Synopsis on the May 10, 2010 Automated Elections. EU-CenPEG Project 3030. 5 October 2010.

Center for People Empowerment in Governance (CenPEG). Praymer: Automated Election System (AES) 2010. Quezon City. 2010. (Published under Project 3030 with the support of the European Union).

De La Salle University College of Computer Studies and Lasallian Justice and Peace Commission. Towards Strengthening Electoral Reforms through ICT: An Assessment of the May 2010 Automated Elections in the Philippines. June 2010.

Dulce, Leon and Rick Bahague. Elections, E-Monitoring, and Empowerment: The Vote Report PH Experience. 4 June 2010. www.VoteReportPH.org.

Jimenez, Evita. Introduction to the EU-CenPEG Project 3030 Report. (Presented at the AES Watch Post-Election Summit. San Juan. 5 October 2010).

Laggui, Drexx. Findings of the IT Forensic Team, 2010 Joint Committee on the Canvass of Votes. (Presented at a Forum on PCOS in AES. Makati City. 5 July 2010).

Locsin Jr., Teodoro L. Chairman's Report on the Committee on Suffrage and Electoral Reforms Hearings on the Alleged Fraud and Precinct Count Optical Scan (PCOS) Machine Manipulation in the May 10, 2010 Automated Elections. House of Representatives, Quezon City. June 2010.

Manalastas, Pablo, presenter of EU-CenPEG Project 3030 report, Main Conclusion; AES Watch Post-Election Summit. San Juan. 5 October 2010.

Muga III, Felix., presenter of EU-CenPEG Project 3030 May 10 Incident Reports; AES Watch Post-Election Summit. San Juan. 5 October 2010.

National Citizens' Movement for Free Elections (NAMFREL). Executive Summary of Terminal Report. Mandaluyong City. 2 July 2010. (found in www.namfrel.org.ph)

Natividad, Marjorie R. Policy Analysis: Digital Signature. MIPOLAW. 18 September 2010.

Ona, Sherwin. Post-Election Summit Report of AES Watch 2010. (Presented at the AES Watch Post-Election Summit. San Juan. 5 October 2010).

Quimson, Bettina. Findings on the Senate Investigation of Antipolo Machines and Hearings of Congressional Committee on Suffrage and Electoral Reforms. (Presented at a Forum on PCOS in AES. Makati City. 5 July 2010).

Roque, Harry. We Want Automated Elections, Not Automated Failure of Elections. (Presented at the AES Watch Post-Election Summit. San Juan. 5 October 2010).

SysTest Labs. Certification Test Report Summary for AES May 2010. Denver. 9 February 2010. (Prepared for the Commission on Elections of the Philippines).

SysTest Labs. Certification Test Report for Source Code Review, Readiness and Security Testing: Philippine AES Voting System. Denver. 9 February 2010. (Prepared for the Commission on Elections of the Philippines).

Technical Working Group on the Random Manual Audit. Report on the Random Manual Audit of the Automated Election System (AES) in the 10 May 2010 National and Local Elections. (Submitted to the Commission on Elections. 20 July 2010)

Vitangcol, Al. S. A Post AES 2010 Evaluation. (Presented at a Forum on PCOS in AES. Makati City. 5 July 2010)

END NOTES

[1] AES Watch is pronounced as "eyes watch".

[2] The conveners and partners of AES Watch currently include University of the Philippines Alumni Association (UPAA); National Secretariat for Social Action of the Catholic Bishops' Conference of the Philippines (CBCP-NASSA), Bishop Broderick Pabillo, National Director of CBCP-NASSA; Bishop Deogracias Iniguez, Head of

CBCP Commission on Public Affairs; Center for People Empowerment in Governance (CenPEG); Ecumenical Bishops Forum; National Council of Churches in the Philippines (NCCP); Dr. Rachel Roxas, Dean of DLSU College of Computer Studies; Dr. Reena Estuar, Chair of Ateneo de Manila University Department of Information Communications System; Dr. Jaime Caro, Chair of U.P. Department of Computer Science; Computer Professionals Union (CPU); Association of Major Religious Superiors in the Philippines (AMRSP); Solidarity Philippines; Philippine Computer Emergency Response Team (PhCERT); Transparency International (TI-Philippines); National Union of Students of the Philippines (NUSP); Engr. Rodolfo Lozada; Health Alliance for Democracy (HEAD); Senior Catholic Citizens' Organization; Association of Schools of Public Administration of the Philippines (ASPAP); Computing Society of the Philippines; Transparentelections.org; Concerned Citizens Movement (CCM); Coordinating Council for People's Development (CPDG); Senior Citizens Organization; Pagbabago (Movement for Social Change); Dilaab-Hearts Foundation; Movement for Good Governance (MGG); Sisters Association in Mindanao; Alyansa Agrikultura; Philippine Computer Society Foundation; Atty. Al. Vitangcol III; NAMFREL; and others.

[3] Comelec provided its response to the issues raised by AES Watch at the 17 December 2009 hearing under cover of its letter to the JCOC dated 4 January 2010. The response did not quell the concerns of AES Watch.

[4] The source code review was done by SysTest Labs of Denver, Colorado, USA, which was the international certification entity contracted by Comelec in October 2009. On 9 February 2010, SysTest Labs submitted an initial report titled Certification Test Report for Source Code Review, Readiness and Security Testing. This report indicated certain areas of weaknesses in the AES voting system but concluded that "SysTest Labs did not find reason to preclude the AES voting system as being suitable for use as an electronic election system" for the Philippines.

[5] This delayed TEC certification of 9 March 2010 was based partly on the SysTest Labs report dated 9 February 2010 (see footnote 4) and partly on SysTest Labs report dated 8 March 2010. The latter report titled Certification Test Report Summary concluded that "findings remain in areas such as documentation, process and setup", that "all issues are considered minor in nature or reconcilable using appropriate manual processes and/or compensating controls" and that "assuming the above mentioned controls are put into practice and that the AES is properly configured, operated and supported, SysTest Labs finds the Smartmatic Automated Election System to be capable of operating properly, securely and accurately and therefore recommends the system for certification and use in the May 10, 2010 election."

[6] There was no indication of the commitment of Comelec to fully adopt the compensating controls recommended by SysTest Labs. The last set of General Instructions for the Boards of Election Inspectors was issued on 4 March 2010, ahead of the 8 March 2010 report of SysTest Labs.

[7] To assure that the source code reviewed was one and the same as that used in the machines, the procedure is to extract the hash code of the software from each PCOS machine and check if it matches that of the copy of the software kept in escrow with Bangko Sentral ng Piipinas. A match is conclusive proof that can be the basis for the assurance. No report was made on the implementation of this procedure during the testing of the machines and, given the time constraint, the procedure was probably not done at all.

[8] Comelec claimed that the hash codes published in its website was erroneous.

[9] The financial information on the three logistics companies was sourced from newsbreak.com.ph.

[10] PPCRV is the Parish Pastoral Council for Responsible Voting, the lone citizens' arm of Comelec.

[11] The TWG-RMA was to be chaired by PPCRV Chair and included the OIC of Comelec Internal Audit Office and the COA Resident Representative in Comelec as members. The COA Resident Representative withdrew as member in March 2010 citing possible conflict of interest and was replaced by the NSO General Administrator in April 2010.

[12] Towards Strengthening Electoral Reforms through ICT: An Assessment of the May 2010 Automated Elections in the Philippines. De La Salle University College of Computer Studies and Lasallian Justice and Peace Commission (June 2010).

[13] For some unclear reason, Comelec disabled the PCOS machine's built-in ultraviolet detector of a ballot security mark. This decision was made at the time the ballots were being printed.

[14] Item 6 of Section 9 (11) says, "The development, provisioning, and operationalization of a continuity plan to cover risks to the AES at all points in the process such that a failure of elections, whether at voting, counting or consolidation, may be avoided."