ANALYSIS OF OUTSTANDING TECHNICAL ISSUES
Executive Summary

The inadequacies and flaws attending the preparations for the May 10 automated election implemented by Comelec with its foreign partner, Smartmatic, were contributory to the glitches and other irregularities that took place on election day and thereafter. The deficient and flawed election preparations, as CenPEG and other citizens groups had warned, became vulnerable not only to technical glitches and other irregularities but also to automated fraud, based on several election protests some of which were studied by CenPEG as well as voters disenfranchisement. Definitely, aside from these weaknesses, the Comelec's claim of "success" should be corrected because AES could do nothing about the widespread vote buying, irregular voters' lists, and election-related violence not to mention allegations of corruption that – in many respects - also affected the conduct of the election including in the local races.

This part of the Project 3030 report presents the highlights of the technical analysis of the automated election system (AES) on its major components and requirements based on the election laws, best IT and industry standards and the principles defined by the AES project – system transparency, accuracy, trustworthiness, and security.

What follows are the highlights of the technical analysis that was consolidated after a long series of consultations, workshops, and further data-gathering of the disturbing trends in the AES. Please refer to the main section on technical analysis for the full text.

1. AES Compliance Issue: TEC Certification

Did the AES operate properly, securely, and accurately?

The 16 facts enumerated below indicate failure of the AES to operate properly, securely, and accurately. While the TEC had issued the mandated certification, it was contingent on the implementation of procedural and technical compensating controls.

On the proper of operations of the AES

Fact 1: Election Returns generated during the Final Testing and Sealing of the PCOS Machines were transmitted to the canvassing laptops at the city/municipal level, the central server, and the server located at the Pope Pius Center.

Fact 2: Some Canvassing and Consolidation System (CCS) laptops failed to print the Statement of Votes (SoV) in some areas and for some contests.

Fact 3: Clustered Precincts - A common experience by voters on election day was having to fall in line for hours under the heat of the summer sun, waiting their turn to vote. While the issue of long queues is not a technical matter relating to the performance of the AES, it nevertheless is part of the whole system. Various groups had warned the Comelec of problems relating to the clustering of precincts resulting in increasing the number of voters per precinct to as many as one thousand voters. The warnings were unheeded, with the long queues resulting in disenfranchisement as some voters simply left the line and never came back.

Fact 4: Transmission Problems - Incident reports indicate that an undetermined number of election returns were conveyed manually rather than through the telecommunications infrastructure.

On the secure operations of the AES

Fact 5: The PCOS machine ultraviolet (UV) mark detection was disabled.

Fact 6: There was no review of the source code of the AES by interested political parties and groups.

Fact 7: Absence of the Digital Signature - Fact 8: The Hash Code extracted from the PCOS Machine is not the same as the one published in Comelec's website.

Fact 9: A Console Port is present in the PCOS Machine and the internal mechanisms, including the software, are accessible by connecting another computer to it.

Fact 10: The CF Card Problem: The CF card problem highlighted the failure of processes in the preparation of the system. The problem also highlighted the process failures within the Comelec with the reactive issuances of memoranda on the handling of the CF card problems in the field.

On the accurate operations of the AES

Fact 11: The voter verifiability feature was disabled or not made available.

Fact 12: The Election Returns generated and printed from various PCOS machines reflected varying date and time stamps.

Fact 13: There were reports of inaccurate counts of the ballot such that the machine count differed from the hand count done by the BEI. In Random Manual Audit (RMA) activities witnessed by the National Citizens' Movement for Free Elections (Namfrel) volunteers noted discrepancies in the machine count of the ballots and hand count. The requirement of accurate ballot counters in the PCOS machine is simply not met.

Fact 14: The number of registered voters in the canvassing system was wrong.

Fact 15: 99.995% accuracy was not met - On July 20, 2010 the Random Manual Audit Team reported a finding of 99.6% accuracy or an error rate of 0.4% (4 marks out of 1,000).

Fact 16: Compensating Controls not fully implemented.

Management and Procedural Issues

It appears that the TEC did not have enough latitude in the performance of its function or that the recommended compensating controls were not fully implemented. The Comelec project time table or calendar of activities was too tight. The Continuity Plan was not properly operationalized as evidenced by the absence of any training and drill exercise.

2. SysTest Labs Certification: What Went Wrong?

SysTest Labs' source code review found many instances of serious programming errors in Smartmatic's programs that may cause, and actually did cause, execution errors on election day, as evidenced by the PCOS program malfunctioning, the PCOS and CCS allowing transmission of FTS results, and a significant number of tabulation errors in the Comelec's public website. Also, SysTest Labs did not test the election design produced by the EMS and the EED for the actual May 10. 2010 election, but only tested the artificially contrived "toy" data supplied by Comelec. Thus there is no way that SysTest Labs could certify that the AES is operating properly, securely, and accurately in accordance with the provisions of RA-9369 because it did not test the AES as it will be used on election day.

To conclude, although the TEC and SysTest certifications revealed serious errors in the source code of the AES, and inadequate security provisions of the AES, such observations could have been arrived at for much less than the PHP70 million that Comelec spent for certification, which was optional anyway.

3. Logistics Issue: Deployment of Machines

The subcontracted firms did not go through the stringent evaluation and review by COMELEC's Special Bids and Awards Committee. They were also not directly accountable to the COMELEC. There was no disclosure on the capability of the subcontracted logistics providers to handle sensitive cargo; and there was lack of information on road networks and mode of transportation.

In terms of security, the Forensic Team identified a vulnerability, the console port on the PCOS, which exposed it to possible breach while in transit or in storage. Forensic Team reported that the shell of the operating system of the PCOS could be accessed by connecting a laptop to it and the operating system does not even ask for a username/password combination.

Even given that the PCOS machines went through quality assurance testing at the Shanghai, China plant, the PCOS machines should have been individually subjected to quality assurance testing at the Cabuyao, Laguna warehouse. The tightened schedule resulting from delays in delivery may have caused the poor quality assurance testing, resulting in, for example, the varying date and time settings of the PCOS machines.

4. Field Tests and Mock Elections

The AES may have been demonstrated to work - but to what degree? Certainly not at 100%. Too many refinements and adjustments were needed to be done to the AES as shown by the problems (such as high ballot rejection rate and transmission delays) encountered in the field tests and mock elections. The field tests and mock elections are a failure.

No time and motion study was conducted by Comelec; neither was there an evident change in management to prepare for the anticipated long queues of voters nationwide. With no sound estimate prior to election day and upon realizing on election day itself that 11 hours is not sufficient Comelec announced late in the day – 3 p.m. – to extend voting time from 6 p.m. to 7 p.m. CenPEG had long raised the issue that 11 hours is insufficient and that voting time should be at least 16 hours or in extreme cases 24 hours to pre-empt massive voter disenfranchisement.

Lesson: The Technical Evaluation Committee should not have certified that the AES is operating properly.

5. Source Code

The right to review/study the source code of the election programs is a right of the citizens as part of the right to information guaranteed by the Constitution and is guaranteed by Section 12 of RA-9369. When the computer does not show how it counts to the public, then the public has the right to review the source code of the computer to check that it is doing the counting correctly. The actual events as they happened before election day, on election day, and after election day proved beyond reasonable doubt that the election computers and the people managing the computerization process made many serious mistakes.

The wrong way can be rectified, with a source code review done by parties independent of Comelec. Comelec did not perform its duty of doing a source code review, since the review done by SysTest Labs did not check the election programs for conformity to our election laws and Comelec regulations.

Furthermore, Comelec exerted its best efforts to avoid releasing the source code to interested political parties and groups for their independent review. On the other hand, CenPEG exerted its best efforts to force Comelec to obey the law as stated in Section 12 (Sec 14) of RA-9369. In the end, the Supreme Court has spoken, and has ordered Comelec to do the right thing.

6. Hash codes

Initial report contained errors; hash codes were of the zipped installable programs, not the programs after installation. No facility was made available on election day for the BEIs and watchers to check whether the program running in the machines is the same as the source code held in escrow at the BSP – to assure the public that the program in the machine is one and the same in escrow – a PUBLIC TRUST issue. It is possible that a different program/software was running on the machines on election day.

7. Digital Signature

The implementation of digital signing in the automated election system is not technically or technologically consistent with the implementation of digital signature technology and is contrary to the requirements of the RFP-AES2010, clarified in the related Bid Bulletin No. 10. The claimed existence of a "machine digital signature" in each PCOS machine is debunked by the findings by SysTest Labs which failed to verify any digital signature as well as the failure of Smartmatic technicians to demonstrate the existence of a digital certificate that will confirm the existence of a digital signature.

The claimed "machine digital signature" does not legally exist. No Philippine law, rule, or statute has accorded legal recognition of "machine digital signature".

Implication: The lack or absence of a digital signature on the ER, SOV, and COC impaired the authenticity and due execution of said election reports. The lack or absence of a digital signature on the ER, SOV, and COC rendered the election reports vulnerable to tampering and manipulation.

8. Technical breakdowns

As predicted, election day was marred with a myriad of technical problems in many clustered precincts. System quality assurance requires that several tests be conducted on the system before it is rolled out to actual operation. The tests include, among others, unit tests, stress test, integration test, full systems or end-to-end tests. If time was properly allocated for the different test activities, many of the problems encountered on election day would have been discovered and properly resolved.

9. Transmission

The exclusion of certain components of the AES from review and certification, specifically the PCOS modem firmware and the non-implementation of Compensating Controls relating to transmission may have rendered the transmission infrastructure vulnerable to attacks or may have allowed the unauthorized access to data/reports for purposes of manipulating the same.

The COMELEC missed the opportunity to validate that all necessary components are in place and are performing as intended by not executing a final and complete dry run of the AES. Had COMELEC done so, the reported errors like varying date/time stamps on the PCOS and the erroneous registered voters count would have been observed and final corrections to the AES instituted prior to election day.

There is a need to conduct a full technical review of the transmission to fully explain the transmission irregularities.

10. UV lamp and ballot security

COMELEC's lack of project management skills and required technical knowledge to understand the intricacies of printing is very evident in its handling of the printing of the ballots and ensuring that the required security feature is present. There was no need to disable the ultraviolet security mark sensing in the PCOS. For disabling the ultraviolet security mark sensing in the PCOS, however, at least PhP30 million of taxpayers' money had to be spent on the handheld ultraviolet scanners. The amount had gone to waste since, as reported by the SWS, only 50% was used. There are also reports that not all handheld ultraviolet scanners had been recovered.

11. Voter's verifiability

Comelec rationalized the disabling of the Cast and Return button in the PCOS by claiming it would cause delay in voting. This deprived the voter of a mechanism to verify that the PCOS computer has interpreted his/her ballot correctly; voter intent may not have been correctly registered in the machine. (Voting delays on E-day were in fact caused by clustering and technical problems and not by the feeding of ballots.)

12. Final testing and sealing (FTS) & CF Card reconfiguration

The May 3 FTS disaster exposed Smartmatic's inexperience in implementing paper-based AES. The actual number (10) of test ballots used during FTS is statistically insufficient to prove that the PCOS machine can correctly credit votes for candidates to the correct candidates.

In the rush to recall, reconfigure, and resend all CF cards, there were reports of delayed delivery or non-delivery of reconfigured memory cards. Contrary to Comelec claims, the reconfiguration was not done mainly at the Cabuyao, Laguna plant but also at DOST provincial offices. Reconfiguration opened opportunities to tamper with the memory cards, CF card switching, and other risks.

13. Canvassing and election results

Faulty programming caused miscalculation of total number of registered voters (Comelec canvassing CCS computer at PICC and Congress canvassing CCS computer) and the high incidence of FTS results transmission. As regards the high incidence of erroneous COCs containing FTS results, it is strongly evident that old faulty CF cards were used on election day. It was also caused by Smartmatic's counting and canvassing system (CCS) program's failure to reject invalid COCs and accept only the valid ones. The program was never subjected to testing and certification in accordance with Philippine election laws – despite the SysTest testing and certification issued by the TEC.