THE CenPEG REPORT ON THE MAY 10, 2010 AUTOMATED ELECTIONS

A Synopsis
EU-CenPEG Project 3030
October 5, 2010

At the OCTOBER PEST (Post-Election Summit) held on Oct. 5, 2010 the Center for People Empowerment in Governance (CenPEG) presented its latest study on the May 10, 2010 automated elections - the first in the Philippines. The October PES was sponsored by the broad citizens' network AES Watch and was held at Club Filipino, Greenhills, San Juan.

The synopsis of that report follows below. The final report - which will cover the automated election system's technical, management, and legal aspects - is due for release this month. The CenPEG study basically finds the Commission on Elections' claim of a "successful" automated election a sham and that the system was vulnerable to widespread glitches and, likewise, favorable for electronic rigging. It challenges the Comelec to prove its claim of "success" and debunk increasing evidence of a possible automated fraud, like pre-loading, by releasing 21 vital election documents - public information - to CenPEG and other citizens' groups and advocates.

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

After months of extensive research – monitoring, observation, documentation, and field case studies – the Center for People Empowerment in Governance (CenPEG) today released its report on the May 10, 2010 automated elections. The **CenPEG REPORT** is being presented at the October PES (Post-Election Summit) convened in cooperation with AES Watch, a broad spectrum of various citizens' watchdogs and advocates that also studied and monitored the automated election.

Among others, **The CenPEG REPORT** consists of incidence reports on the election and an analysis of the AES's various components particularly technical and management. The full and final report – including the legal study - will be released within weeks after the October 5 post-election summit.

CenPEG's Project 3030 report is based on extensive research that involved the following:

- Project 3030 Monitoring of Election Incidents (May 2 – 31, 2010)

- Extensive Case Studies conducted in 9 provincial areas (with informants from Comelec, BEIs/BOCs, DOST, Smartmatic-TIM ITs, PPCRV volunteers, voters, and others)
- Consultants and expert analysis from the disciplines of IT (computer studies and science, security, programming), policy analysis, law, public administration, business, mathematics, Geographical Information System, anthropology, among others
- Project research coordinators in 12 regions
- Thousands of trained poll watch volunteers in at least 50 provinces
- 18 student volunteers from UP (Manila and Los Banos)
- AES Watch monitoring volunteers
- CenPEG Project partners like CPU, NCCP (People's International Observers Mission); Citizens Election Monitoring (CEM) group, bloggers, and others
- CONCORD / Healing Democracy election monitoring in Mindanao
- Eastern Telecommunications (for the electronic services) and media (for additional reports)

This **CenPEG Report** is based on a study undertaken by CenPEG titled "EU-CenPEG Project 3030: Action to Protect the Integrity of the Vote and Transparency in the 2010 Elections." It is the sixth of a series of studies made by the policy research institution since the August 2008 ARMM automated election until today. Taking off from the "30-30 Vulnerabilities and Safeguards," CenPEG's 2-year study aims to deepen the understanding of the automated election system's 30 identified vulnerabilities and propose corresponding 30 safeguards and safety measures as a mechanism for protecting the integrity of the vote and transparency in the 2010 elections in accordance with its policy research and advocacy program. It covered the critical technical, management, and legal components of the automated election system. The findings and policy recommendations of this and other studies will be the subject of advocacy in our engagement with Congress, Comelec, and other institutions.

Highlights of the new report follow:

I. WHAT HAPPENED ON ELECTION DAY?

PCOS malfunctioning, breakdowns

In many precinct incidents across the country, late deliveries, malfunction and shutdowns, unreliable back-up batteries, and equipment shortage marred the disposition and operation of PCOS machines thus causing delays in the opening of voting, counting, and the whole election day process itself.

Defective compact flash cards

Delays in the delivery of reconfigured CF cards (in some cases, absence or loss of the memory cards) and using defective memory cards figured in the high-incidence reports, delaying FTS and voting, or absence of FTS. A high percentage of CF cards being brought manually to canvassing, and precincts resorting to manual voting were also reported. In many cases, this problem also resulted in failure of elections or in electoral protests involving the manipulation of CF cards.

Thermal Paper

The use of unofficial thermal paper was registered as a high incidence across the country. In such cases, as explained by local Comelec officials, the official thermal paper was used up during the FTS. Still, questions remain where those unofficial thermal papers – whose lifespan will be shorter than the 5 years promised by the tech provider - came from thus further casting doubts on the security and accuracy of the election results.

UV scanners

Verifying the authenticity of ballots was not fully implemented as provided by law with the non-use of UV scanners by a significant number of precinct BEIs. (Based on the SWS survey, only 50% of BEIs used the ballot scanner.) There were reports of precincts not receiving any scanner at all; BEIs who received it either left the scanners untouched or widely mistook them for emergency flashlights.

Irregularities in voting procedures & voter disenfranchisement

The lack of change in management was evident in Comelec's failure to put in place an effective voting system for the projected long queues of voters as a result of precinct clustering. What actually happened was near-anarchy as dramatized by conflicting procedures, violations of voting instructions, buildup of long lines due to technical hitches, and intimidation by politicians and supporters.

Minus the presence of PCOS machines, election day preserved the traditional forms of election cheating marked by violence especially in many hot spots. The voting turnout based on Comelec's 75% - which Project 3030 estimates as conservative – was the lowest in national elections since the 1986 snap polls.

Transmission snafus

The fact about extensive transmission glitches – not simply an isolated case – shows an unsound decision to enforce an election technology when the required telecommunication infrastructure is unreliable. The satellite contingency hit snags.

With incidence reports showing the unexplained stoppage of transmission at certain hours, Comelec should explain credibly its claim of fast transmission of election results at the national servers when voting delays and transmission glitches taking place at the precinct and municipal levels nationwide may prove otherwise. There should be a full disclosure of transmission operations and data by the election managers.

Canvassing connectivity problems and discrepancies

The widespread mismatch of time stamps, discrepancies in audit logs, and canvassing print logs make the audit mechanism provided by Smartmatic-TIM unreliable and unsecure. Like the precinct-level failures, many municipal canvassing centers also had transmission glitches that obstructed transmission of canvassing results to the provincial and national canvassing.

Numerous reports of provincial COCs containing FTS results show the CCS program did not undergo testing and certification.

Vote buying, violence & other irregularities

Other widespread irregularities were vote buying ("the most rampant in several years"), ballot pre-shading, and flying voters. There were many incidents of police and military personnel inside voting centers contrary to law. Election-related violence was perpetrated by private armed groups resulting in failure of election in many areas. Military and other security forces were also involved in reports of vilification campaigns against some Partylist groups and militarization in the rural provinces intimidating many voters.

ELECTION PROTESTS

The lack of safeguards and security measures made the AES vulnerable to automated fraud particularly in a country where cheating of various types persists as a norm during elections. Comelec records show at least 100 election protests from 41 provinces and cities by June 2010 have been filed.

Many election cases apparently involved the complicity of certain Comelec officials, BEI members, and others. In at least one case, allegations about the tampering of CF cards have been given credence in the Pasay City election protest with Comelec ordering a recount of the votes for the mayoralty contest.

II. THE STATE OF ELECTION READINESS BEFORE MAY 10

Board of Election Inspectors (BEI)

Training for the BEIs was insufficient making them unprepared for managing crowd control, systematically implementing new voting procedures, or even technical troubleshooting when circumstances forced them to.

Smartmatic-TIM IT technicians

Technical operations, maintenance, and troubleshooting were hampered by the hiring of many non-IT technicians; shortage of technicians in many precincts (some handling 10 clustered precincts); inadequate training and low pay.

Voter education

Voter education called on the voters to become hostage to the un-friendly, burdensome demands and rigors of the machine, not the other way around. The law says the adopted technology should be compliant with the "actual conditions" of the country, which includes a political culture aligned with modern technology.

Capability and readiness of the AES machine technology

The manufacturing of PCOS machines was delayed thus undermining quality assurance. The Smartmatic-TIM PCOS technology is the lowest end in the international market with limitations and disabled features (such as voter verifiability) that put undue burden to the voter with his/her rights violated; the fact that the machine is prone to tampering was hidden from the public.

Forwarders for election paraphernalia deployment

There was lack of transparency in the hiring of 3 logistics companies (public bidding), and in their papers, operational plans, and subcontracting. Project 3030 incident reports showed delays in the deployment of election paraphernalia and the possible risks involved in the delivery.

May 3 final testing and sealing (FTS)

The May 3 FTS fiasco involved the mismatch between CF cards and ballot designs but there were extensive reports as well of PCOS malfunctioning, missing SIMs, transmission glitches, problems with back-up batteries, etc. The FTS showed both Comelec and Smartmatic-TIM were ill-prepared for the automated election, management-wise.

Electronic transmission

Comelec's and Smartmatic-TIM's grasp of the power, road network, and transmission infrastructures that are critical to the success of the automated election should be challenged. Either they over-estimated the infrastructure capabilities or simply did not do their work in this field.

Mock elections and field tests

The mock elections and field tests, aside from suffering delays, did not simulate the actual conditions as required by law. As a result, they failed to anticipate the widespread election-day long queues of voters and technical hitches with viable contingency measures.

Ballot delivery

Aside from the issues involving the design and printing of ballots that compromised the ballots' integrity and security, incident reports showed numerous problems including wrong deliveries and dangers with regard to storage and safekeeping.

"Fast results"

Just to conclude this portion: Actual voting in the automated election was by several hours – compared to the previous manual system. Mr. Aquino III was proclaimed as President on June 9, 2010 – 30 days after the May 10 election; Mr. Estrada was proclaimed on May 30, 1998 – only 19 days after the May 11, 1998 election. The election turnout in the May 2010 election is 75% (which is conservative) – the lowest in 24 years of presidential election. What then is the basis of the claim of "fast" results, quicker voting, and more voters voting under AES?

OTHER RELATED REPORTS

People's International Observers Mission (PIOM): In a public statement May 15, 2010, the 86-member People's International Observers Mission (PIOM) found the first automated election in the Philippines "far from being fair, honest and peaceful. "The widespread intimidation, vote-buying, corruption and violence showed that automation could solve only part of the problem," PIOM stated. "In focusing on the machines, the Comelec [Commission on Elections] lost the people."

Consortium of Christian Organizations for Rural-Urban Development (CONCORD): CONCORD, in its Healing Democracy report based on monitoring and documentation of the ARMM and Lanao del Sur elections described the May 10, 2010 election as "no different from previous fraudulent, anomalous, and violence-ridden polls in the country." CONCORD said, like in previous elections, "Comelec should explain for the technical glitches, transmission failures, as well as incidents of fraud and violence taking place across the country."

Committee on Suffrage and Electoral Reforms (CSER), House of Representatives: In its June 2010 report, the House Committee on Suffrage and Electoral Reforms (CSER), concluded, "On the national level, our (committee's) assessment is of a mixed success. Automation showed no substantial advantage. On the local level, our assessment is profound unease." The CSER reminded: The goal of automation was never two-fold: speed and accuracy. "It was always singular: accuracy." Among other disturbing issues, the committee noted: Anomalies in time and stamp in various election returns (ERs); the May 3 FTS fiasco; the "curious distribution" of blank extra CF cards with two burners per province; the disenfranchisement of 3 million voters; cheating on the local level.

III. TECHNICAL ANALYSIS

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. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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 of full technical review of the transmission to fully explain the transmission irregularities.

8. **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 PhP30million 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.

9. 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.)

10. 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.

11. 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.

IV. Synthesis and Conclusion

Were the election day incidents as reconstructed isolated or did these happen on a small-scale or only in areas covered by Project 30-30 research? Were these incidents mainly caused by clerical or simple mathematical miscalculations or were these simple reports of technical glitches fabricated by "misinformed minds?"

If these were only isolated and treated as minor glitches, what explains the following disturbing findings that occurred NATIONWIDE and were validated again in congressional hearings, investigations and Project 3030 case studies?

- Mismatched time and date stamps on all PCOS machines;
- Transmission failures;
- Erroneous COCs in at least 57 provinces and cities;
- Ballots and CF cards delivered manually for canvassing;
- Discovery of the console port in all machines making the PCOS vulnerable to tampering;
- Erroneous entries of total number of voters and votes cast in the national canvassing center and Congress;
- Near anarchy at the clustered precincts;
- Not to forget the pre-election incidence of defective CF cards

All of these have tainted the integrity, credibility, and accuracy of the PCOS machines and the election system.

Based on CenPEG research that includes testimonies of Comelec officials, other election personnel like the BEIs, Smartmatic IT technicians, poll watchers and voters as confirmed and validated by House hearings and investigations conducted by independent IT groups, other election watchdogs and media reports – the magnitude of these problems was nationwide. There was high incidence and widespread occurrences of the technical and management problems. Based on available information, data and documents, the "rousing success of the AES" as claimed by Comelec is therefore without material basis.

Moreover, blunders in the automated election system implemented on May 10 can be traced to decisions made by the Comelec and its contractor Smartmatic-TIM to sidestep accuracy, security, and transparency standards on both hardware and software technologies needed to ensure reliable and credible election results. All these and more made the automated election vulnerable to all forms of cheating including ballot pre-shading and possible pre-loading of election data.

The challenge of establishing solid proofs and empirical data to prove automated cheating – including a possible pre-loading - whether wide-scale or systematic and establish in no uncertain terms the possible accountability of Comelec has been hampered precisely by the national poll body's unexplained refusal to disclose vital election documents – all 21 of them – that were long requested by CenPEG and other citizens' groups. The disclosure of these documents will also help test and validate Comelec's claims of election "success" and dispel increasing allegations of electronic rigging. The more intransigent Comelec is in refusing to make this public information available especially for worthy causes like research without preconditions or under "controlled environment" the stronger public concerns there will be that the poll body is hiding something.

CenPEG is optimistic that answers and clarifications on the questions and doubts about the accuracy, trustworthiness, and security of the PCOS and the whole election system can be discerned from the 21 public documents it has requested but which were denied perfunctorily by the Comelec en banc last July 26, 2010.

In the meantime, Comelec should be made to explain why its implementation of the election automation was inconsistent with major provisions of the Philippine Constitution (voter rights, public information, government-citizens partnership in governance, etc.), RA 9369 and other election-related election laws.

Comelec should also explain in unequivocal terms why at the first instance it chose to outsource the Philippines' automated election to a foreign company – under still non-transparent transactions at that – that proved to be ill-equipped and ill-informed of the country's election conditions instead of tapping the Filipino IT industry whose skills and competence are comparable with IT giants in the world.

How easily the Comelec must have forgotten that elections are the sovereign act of a sovereign country and that, as the 1987 Philippine Constitution itself provides: "The State shall give priority to research and development, invention, innovation, and their utilization; and to science and technology education, training, and services. It shall support indigenous, appropriate, and self-reliant scientific and technological capabilities, and their application to the country's productive systems and national life." (Article XIV, Section 10)

EU-CenPEG Project 3030
www.eu-cenpeg.com; www.cenpeg.org