

# 30 Vulnerabilities and Safeguards VS Cheating in the AES 2010

A Must for  
VOTERS' EDUCATION  
and POLL WATCHERS GUIDE  
for the first nationwide  
Automated Elections in the Philippines



**Center for People Empowerment in Governance (CenPEG)**

[www.cenpeg.org](http://www.cenpeg.org); Email: [cenpeg.info@gmail.com](mailto:cenpeg.info@gmail.com); [info@cenpeg.org](mailto:info@cenpeg.org)

3/F CSWCD Bldg., University of the Philippines  
Magsaysay Avenue, Diliman, Quezon City 1101 Philippines  
Tel/Fax +9299526

# **30 Vulnerabilities & Safeguards in the AES 2010 : Promoting the Integrity of the Vote\***

## **INTRODUCTION**

The Automated Election Law (RA 9369) is a landmark legislation aimed at modernizing the election system in the Philippines. Not only does it recognize the need to pilot test the technology to be used before going full blast, it also ensures that the technology chosen should be “suitable to Philippine conditions.” It may have its own vague provisions such as Sections 30 down which still refer to manual elections, but over-all it is a law that is unique in that it provides major safeguards to help ensure the integrity of the vote, promote secret voting yet transparent and credible counting in the poll automation – in short, to make election a mechanism for making democracy work. Comelec, meanwhile, has only to comply with the law’s distinct provisions of safeguarding the elections in May 2010 to avoid the dangerous pitfalls of automated disaster.

The country’s prime election manager, the Commission on Elections (Comelec), sees the automation of elections as the answer to fraud and is also widely perceived by the public as guaranteeing clean elections in 2010. While automating the elections claims to give advantages such as speed and accuracy in tabulation, it can still lead to wholesale cheating if safeguards and security measures are not properly implemented especially in the counting and canvassing stages. In fact, modernizing the election system without substantially addressing systemic election fraud and dismantling the powerful cheating machineries that have also affected the Comelec organization will make the use of modern technology futile. A machine is “cognitive neutral” and it works as commanded by its operators – or manipulators. It needs the proper political environment to function well.

The whole AES process has 30+ vulnerabilities that the Center for People Empowerment in Governance (CenPEG) initially identified and also looked into by the Automated Election System (AES) 2010 Policy Study under the Dean’s Office of the University of the Philippines’ College of Law through painstaking studies. These phases in the AES process have been deemed vulnerable because these are where either cheating can take place or unclear rules of procedure and continuity plan lead to chaos or failure of elections. The vulnerabilities range from ballot printing, warehousing and delivery of machines, hardware and software deficiencies, voting, counting and electronic transmission of votes; to canvassing and proclamation of winners in 2-3 days.

These problems are largely due to Comelec’s own lack of capability to manage the AES and misinterpretation of RA 9369 (Automated Election System Law). As of this writing, certain provisions of RA 9369, such as the pilot testing of machines in 2 highly-urbanized cities (HUCs) and 2 provinces each in Luzon, Visayas, and Mindanao, as well as the source code review, have not been complied with. Added to this, are the serious questions regarding Comelec’s and the Comelec Advisory Council’s (CAC) information technology (IT) competency which impacts how these bodies handle, manage, and properly decide about the AES for 2010 which will use Smartmatic’s SAES-1800 (Smartmatic Auditable Election System) for counting and the REIS (Real-Time Electoral Information System) for canvassing. With their lack of proper IT competency, Comelec should seek wider consultations from various Filipino IT groups regarding the AES and SAES-1800 especially expert users groups of Linux which is the operating systems to be used in the AES May 2010 elections.

Furthermore, Comelec is already implementing the RA 9369 in the absence of Implementing Rules and Regulations (IRR) which they should have crafted immediately after the law was passed as well as the adjudication process of resolving electoral protests which should have been drafted by midyear to give time for legal minds to study. In light of this, Comelec should immediately publish its IRR so that political parties, poll watchdogs, and the general public are made aware of how Comelec will actually implement the AES and how it plans to deal with potential problems. Data for this list of vulnerable spots that should be plugged with proper safeguards are culled from months of studying Comelec’s actions and decisions regarding the AES, a critique of the RA 9369, observations of the bidding procedures, and technical assessment of the Request for

Proposal/Terms of Reference and available literature regarding the machines. Consultations and workshops with IT professionals and lawyers were conducted to consolidate the data gathered.

The Comelec has revised the AES timetable six (6) times since April 2009 and each time, preparation for every activity is either shortened or removed altogether, e.g. the April 2010 ARMM election. Rushing and shortcutting the preparations without sufficient safeguards in place will endanger or worst spell “30” or finish to this P7.2B single biggest major election project in the world. It is the aim of this document to suggest interventions and safeguards for Comelec to adopt for each of the identified vulnerability and help ensure the integrity of the vote and transparency of the elections in May 2010. It is hoped that this matrix may serve as a “wake up” call for Comelec to be realistic and stop harboring illusions about the so called “dream polls” that will decide the next President, Vice President and other national and local leaders in 2-3 days. If the AES pushes through without the major safeguards in place, may this document serve as a guide and alert mechanism for poll watch groups, advocates for credible and peaceful elections, political parties and well-meaning candidates with regard to the vulnerable areas of the AES that they should guard and watch out for with greater vigilance, courage and devotion

This paper is being published in the interest of voter’s rights, the people’s right to public information, as well as government transparency and accountability. Permission is granted by the Center for People Empowerment in Governance (CenPEG) for the use of this paper for research, analysis, public policy discussions, forums, and media reports with proper attribution to its publisher. CenPEG, an independent policy institute which is duly registered with the Philippines’ Securities and Exchange Commission (SEC), reserves its copyright use and all legal remedies that it implies. CenPEG has been an official observer in Comelec’s bidding and procurement procedures, as well as in the Senate Committee on Constitutional Amendments which also conducts hearings related to the automated election.

For other papers, publications, and downloadable reference materials and PowerPoint presentations, please see [www.cenpeg.org](http://www.cenpeg.org) and [www.aes2010.net](http://www.aes2010.net).

August 28, 2009

Center for People Empowerment in Governance (CenPEG)  
[www.cenpeg.org](http://www.cenpeg.org); Email: [cenpeg.info@gmail.com](mailto:cenpeg.info@gmail.com), [info@cenpeg.org](mailto:info@cenpeg.org)  
3/F CSWCD Bldg., University of the Philippines  
Magsaysay Avenue, Diliman, Quezon City 1101 Philippines  
Tel/Fax +9299526

	<b>Period</b>	<b>Activity/ Vulnerability</b>	<b>Why is it vulnerable?</b>	<b>Intervention</b>
1	Pre-Election	Testing of the lowest calculated bidder's system during the bidding	<p>There was inadequate and at times improper testing of the Smartmatic SAES-1800. For instance, the battery test was conducted on a PCOS machine that was on stand-by but still its wiring failed. Furthermore, the tests were done in a controlled environment and were not able to prove that the system will be able to handle prevailing conditions in local areas because of the lack of a rigorous stress test in actual conditions.</p> <p>Aside from this, the internal system particularly those pertaining to the integrity and security of the data as well as source code were not discussed or scrutinized. There was also no disclosure of the full technical specifications of the SAES-1800 that would have given the Technical Working Group, Comelec Advisory Council and observers adequate knowledge of the system's capabilities and weaknesses.</p>	<p>The SAES-1800 should be re-tested in conditions that reflect the prevailing conditions in local areas. There should also be adequate stress tests as well as discussions and scrutiny of its internal system including its data integrity and security features as well as source code. Additionally, Comelec should immediately make available the full technical specifications of SAES-1800 to allow independent IT professionals to scrutinize the system's capabilities.</p> <p>Proceedings (including video and photo) of the bidding process and profiles of the winning bidder should also be made available for public scrutiny or evaluation.</p> <p>In addition, Comelec should compel Smartmatic-TIM to disclose its real affiliations, home base, connections with certain politicians, etc. so that its political neutrality can be ascertained.</p> <p>Only when these are done can the public properly gauge if the SAES-1800 will be able to perform well in 2010.</p>
2	Pre-Election	Proprietary nature of the source code of the PCOS and CCS machines	<p>The source code is the human-readable version of the computer programs running on the PCOS and BOC computers. The source code will help us fully understand how the machine and the CCS software will work. Aside from how the votes are tallied, we can see from there how the security measures are instructed to the machines. Among the instructions contained in the PCOS source</p>	<p>Comelec should immediately release the source code to interested parties and explicitly put the source code review process in its timetable.</p> <p>Smartmatic-TIM should also make available the complete technical documentation of the AES</p>

			<p>code is how votes are counted. The source code will therefore reveal whether the counting and canvassing are done properly (e.g. Vote for X candidate is counted as 1 and not as 2).</p> <p>RA 9369 requires Comelec to provide the source code to all interested parties. The law states that “Once an AES technology is selected for implementation, the Commission shall <b><u>promptly make the source code of that technology available and open to any interested party</u></b> or groups which may conduct their own review thereof.”</p> <p>Without a review of the source code the public will never know if malicious codes capable of cheating in the programs are present or not.</p>	<p>including security architecture and other design documents.</p> <p>Smartmatic-TIM should also compile a virtual machine image with a full build environment and all source code together with all the compilers and tools that are needed to build the code.</p> <p>Comelec cannot repeat what it did in the ARMM 2008 elections when the source code was not reviewed due to “time constraints.”</p> <p>Comelec should therefore subject the source code to review so that errors and bugs are corrected and malicious codes capable of cheating in the programs are eliminated.</p> <p>A set of guidelines should have been crafted earlier to ensure the prompt and proper review of the source code.</p>
3	Pre-Election	Compiling or converting of reviewed and approved source code into a machine-executable format	<p>Once the source code is reviewed and approved (provided that all modifications recommended by the reviewers in accordance with RA-9369 and the Comelec ToR are incorporated into the final source code), it will then be compiled or converted into a machine-executable format which will be burned in each PCOS machine or installed in each CCS machine.</p> <p>Without transparency in this process of compiling and converting the source code into a machine-executable format, there is a possibility that they will convert or compile the wrong source code into the machine-executable format and thereafter installed in each PCOS and CCS machine and run the elections in 2010. If this</p>	<p>After the program has been reviewed, approved, and digitally-signed by the TEC, the compilation of the source code to machine-executable programs should be made transparent to all political parties and poll watchdogs. This can be conducted in a large hall with all political parties present allowing them to watch the program developers compile the source code into machine-executable version.</p> <p>After compilation to machine executable program, the SHA256 hash value of the machine executable should be computed, and the computed value printed out and given to all political parties. The watchers of the political parties can then use these printouts</p>

			happens, the public will not know what the programs do, because the compiled codes are not from the reviewed programs.	on election day to confirm that the approved program is actually loaded into the PCOS and CCS computers.
4	Pre-Election	Burning or installation of the programs into the firmware of each PCOS machine to be done at the factory in Taiwan (from September to November, 2009)	Comelec does not have a plan on how the integrity of the program installed in each PCOS machine will be verified. In the absence of this important verification process there is a high likelihood that the wrong program will be installed in some of the 82,000 PCOS machines to be manufactured.	Comelec should provide the Board of Election Inspectors (BEIs), political parties, and poll watchers with a copy of the SHA256 hash value of the machine executable compiled from the approved program. On election day the SHA256 hash value computation should be performed on each PCOS machine and its hash value printed in the initialization report to be checked by BEIs and poll watchers. The hash from the approved programs as well as the hash from each PCOS machine should match to ensure that the approved program is running in each machine. If the values are different from the hash of the approved program, the wrong program was installed in the machine.
5	Pre-Election	Preparation of the final list of voters, candidates and precincts	<p>If the lists are not properly monitored, there is a possible manipulation of Voters' List that can lead to massive disenfranchisement. The Candidates' List should also be closely monitored so that all eligible candidates are included. This list will be used to configure each ballot; therefore, if the candidate's name is excluded from the list, s/he/they will not be in the ballots and will surely lose in the elections.</p> <p>The Voter's List is very important because the AES does not solve the flying voters' problem.</p>	Poll watch groups and political parties must scrutinize closely the voters and candidates list to ensure that there is no disenfranchisement. Comelec must also publish the names of the 4 million voters it reportedly purged from the voters list since March this year in at least 2 major newspapers.
6	Pre-Election	Printing of ballots Outsourcing of printing of ballots	After the voters list, candidates list and project of precincts are finalized, these are then converted by Smartmatic-TIM into ballot images unique for each municipality because local candidates differ from one	Comelec should make public its plans regarding the printing of the ballots. In particular, it should have an accurate accounting of how many ballots are spoiled and how many ballots are valid during

			<p>municipality to the next. This ballot image will then be forwarded to the National Printing Office or Bangko Sentral ng Pilipinas for printing.</p> <p>However, if the NPO or BSP does not have the capability to print these ballots because of the security markings (e.g. bar codes, hologram, micro-printing, etc) required for each ballot, they can issue a certificate to Comelec stating that they are unable to print these ballots. If this happens, Comelec can outsource the printing of the ballots to a private company.</p> <p>One possible scenario in the printing of the ballots is that excess ballots might be printed despite RA 9369 clearly stating that only 3 excess ballots will be printed per precinct. These excess ballots could then be pre-marked/pre-shaded and used as legitimate ballots during voting in favor of certain candidates.</p> <p>Add to this, the identity of the private printing company, should its service be utilized, should be immediately made available to the public. In particular, it must not have any dubious political connections to dispel the fears of manipulation of the printing of ballots.</p>	<p>printing to lessen the probability of excess printing. This information should be made available to poll watch groups and political parties.</p> <p>Additionally, it should be transparent in its choice for a private printing company in the event that NPO and BSP are unable to meet the printing requirements of RA 9369.</p>
7	Pre-Election	Storing of ballots Packing of ballots Shipping of packed ballots	<p>The storage of the 50 million ballots is done by Comelec until the time of delivery. Without adequate security measures, pre-shading/pre-marking of ballots is a likely scenario. In the PCOS-OMR voting, watchers and BEIs will not be able to detect if a ballot is marked by only one person since unlike in the manual voting where the voter writes the name of the candidate, this time around the voter will just shade the oval corresponding to the candidate's name. Theoretically, one person can shade</p>	<p>Comelec should make public its plan regarding the storing, packing and shipping of ballots so that poll watch groups and political parties will be able scrutinize if these plans would ensure the security of the ballots. These include indicating who will do these important steps in the election process. The poll body should also put in place punitive measures to persons who will be found in possession of unsecured ballots prior to election day.</p>

			<p>more than one ballots without his/her handwriting being detected.</p> <p>The same security concern is raised during the packing of ballots. Packing of the ballots is according to city and municipality but bundled according to precincts. Adequate security measures should be put in place so that these ballots are properly packed according to precincts and will not fall into the hands of unscrupulous persons.</p> <p>After the ballots are packed these will then be shipped to corresponding municipalities. The chosen shipping company by Smartmatic-TIM is 2Go of Aboitiz. Again, the same security concern is raised during the shipping of ballots. Add to this, there is serious concern regarding the political neutrality of the Aboitizes who are allegedly linked to First Gentleman Mike Arroyo.</p> <p>Another possible issue is the earlier date set for the delivery of ballots and also of other activities (i.e. setting of configuration, testing of the machines against the actual configuration with the ballots; deployment of machines, setting up of transmission sites, training of operators and checking, demos and sealing of machines before shipping) for the ARMM elections.</p>	<p>Comelec should also explain why activities for ARMM elections are held earlier than the rest of the country.</p> <p>Poll watch groups and political parties should have an effective monitoring system of the printing, storing, packing, and shipping of ballots making sure in particular that the correct numbers of ballots are printed and that these have the proper security markings.</p>
8	Pre-Election	Configuration, installation, deployment and designation of servers	<p>A server is a computer that stores application and data files for all workstations on a network. It is not only an issue of transmission. It also involves housing/storing the data, handling requests for data, file transfers and other network services from other computers. So whoever is controlling the server has the potential power to control what data he wants to store as well as what data he wants to transfer.</p>	<p>Deployment of multi-level server is the ideal way to go to have a better check and balance mechanism on what data is being requested and transmitted.</p> <p>Proper data security measures should be implemented to avoid data manipulation by unauthorized users. If the data is not encrypted (see #22), the data can be altered during transmission and in the BOC machine.</p>

9		Configuring the machine – A compact flash card is inserted into each PCOS machine to configure it to read a specific ballot image	<p>Each municipality has a unique ballot image because the names of candidates for local contests differ for each municipality. This ballot image is saved in a compact flash (CF) card which will be used to configure each PCOS machine to read a specific ballot image on election day.</p> <p>Election results can be manipulated by pre-populating the CF cards with deceitful data.</p>	<p>Comelec should have a clear plan as to how it will secure 82,000 compact flash cards containing ballot images that each PCOS machine will read.</p> <p>Poll watch groups and political parties should monitor the security and integrity of the CF cards.</p>
10	Pre-Election	Preparation of transmission sites/infrastructure	<p>The whole AES relies on adequate and reliable transmission infrastructure for the transmission of election returns from the precinct to various canvassing centers. Without a good transmission backbone that can handle the transmission load on election day, transmission failure and connectivity failure can happen.</p> <p>Aside from this, there is also a possible scenario of denial of service attack wherein the transmission lines will be flooded by a big load of data momentarily paralyzing the whole transmission, or transmission sites being physically attacked to cut off signal in a particular area.</p>	<p>Comelec should be clear regarding the realistic condition of transmission infrastructures in the country as well as the possible network traffic on the day of elections. It should also come up with a Geographic Information System (GIS) mapping and analysis of various infrastructures such as telecommunication, road and power infrastructures before it came out with the adoption of the PCOS technology for the 2010 elections. The GIS is vital to ascertaining the feasibility of the chosen technology to deliver clean, credible, and transparent elections in May 2010.</p>
11	Pre-Election	Deployment of machines	<p>As with the shipping of ballots, machines will also be deployed using the services of 2Go of Aboitiz. The 82,000 PCOS machines will be first stored in a central warehouse located in Malolos, Bulacan, a known hotspot for criminal activities. It will then be deployed to various hubs and sub-hubs all over the country before reaching the cities and municipalities.</p> <p>From here machines will be deployed to thousands of voting centers through various transportation means, including loading the machines on top of carabaos and crossing rivers as what happened during the ARMM 2008</p>	<p>Comelec should explain its plans regarding the deployment of machines. In particular, it should justify its choices for hubs and it should also paint a realistic picture of how these machines will be transported to various parts of the country. Again a GIS analysis would have aided the poll body in doing this.</p> <p>Poll watch groups and political parties should have an effective monitoring system regarding the deployment of machines in different parts of the country.</p>

			<p>elections. Without sufficient stress tests conducted during the bidding process, it will be difficult to gauge how the machines will perform after going through the wear and tear of deployment that would characterize many of the voting centers in the country.</p> <p>Aside from this, the security plans for the deployment of machines is also unclear. While in the manual system ballot box snatching is prevalent it is possible that PCOS machine-snatching could happen in the 2010 automated election.</p>	
12	Pre-Election	Testing and sealing of machine 3-7 days prior to voting	<p>Around three (3) to seven (7) days before Election Day, all PCOS machines will be subjected to final testing and sealing by the BEIs, candidates' representatives and citizens' arms watchers who shall vote with blank test ballots, then manually counted and compared with those machine counted.</p> <p>The BEIs, candidates' representatives and citizens' arms watchers will then sign a certification document before the machines are sealed and kept again for at most a week before election day.</p> <p>The long lapse of 3-7 days between the testing and sealing of machines and actual election day is a vulnerable spot. During this period the machines will be stored in the municipal or city treasurer's office. With cheating machinery still intact all over the country, there is no way that this opportunity can escape the cheaters' magic.</p>	<p>Full 24-hour monitoring, if possible by CCTV, of the stored and sealed machines should be instituted by Comelec in each of these storage places.</p> <p>The certification statement should also be made public as this could be problematic given the lapse between testing and sealing and actual day of elections.</p> <p>Days before election, Comelec should provide security to thousands of teachers who will man the BEIs.</p>
13	Election day	Preparation of election paraphernalia (ballots, machines, voters' list, etc) Breaking of seal of machines	BEIs will prepare election paraphernalia prior to the opening of polls at 7 a.m. Possible problems at this stage in the election day include:	Comelec should have a viable continuity plan should any of these scenarios happen.

			<ul style="list-style-type: none"> <li>- The voting center is flooded</li> <li>- The seal is broken or there is no seal</li> <li>- Machines have been physically hacked or water logged</li> <li>- Security threats – civil disturbance, terrorism threats</li> </ul>	Poll watch groups and political parties should monitor the transfer of election paraphernalia from the treasurer’s office to the voting centers.
14	Election day	BEIs insert a physical key into the machine to power it	<p>At 7 a.m., the BEIs will insert a physical key into the PCOS machine to power it. Possible problems at this stage on election day include:</p> <ul style="list-style-type: none"> <li>- Power failure</li> <li>- Hardware failure</li> </ul>	<p>Comelec should have a viable continuity plan should any of these scenarios happen.</p> <p>Poll watch groups and political parties should monitor the actions of the BEIs at each step of the voting day.</p>
15	Election day	BEIs type their passwords	As what happened during the ARMM 2008 elections, the BEIs might forget their passwords causing delays in the voting process.	Comelec should have a viable continuity plan should this scenario happen. However, any assistance should be properly monitored and recorded.
16	Election day	BEIs initialize machine and print initialization report to show zero votes have tallied in the machine	<p>The RFP/TOR does not require the initialization report to show that there are no ballot images stored in the machine and that the proper program was burned into rom and ran in the machine.</p> <p>It is therefore possible, especially if the source code is not reviewed, that there are already stored ballot images in the machine prior to voting but which has not yet been tallied and therefore can still be included in the ER.</p> <p>Furthermore, without a proper data integrity verifier (i.e. hash function), there is no way to ascertain if the program installed in the machine was the program reviewed and approved.</p>	Comelec should include in the initialization report proof that there are no ballot images stored in the machine already. Additionally, it should also require the printing of the hash of each machine for verification by the BEIs and poll watchers and immediately subject the source code to review.
17	Election day	Voter fills in ballot with up to 300 names font size 10 on each	When the voter fills in the ballot these possible scenarios can arise:	Adequate voters’ education should be given by Comelec and other concerned groups, not just the

		side of the ballot that is as long as 30 inches or about 2 ½ feet - Long ballot	<ul style="list-style-type: none"> <li>- Ballot gets wet, crumpled, smudged, or incorrectly-filled</li> <li>- BEI or other persons assist voter – if done improperly, this may violate secret voting principle as what happened in many incidents during the 2008 ARMM poll</li> <li>- Font size, long ballot, and numerous names unfriendly to disabled, illiterate, ethno-linguistic minority, and elderly</li> </ul>	<p>endorsers of the AES but also by those who are critical of it.</p> <p>The BEIs should also be strict in implementing the principle of “secret voting.”</p>
18	Election day	Voter feeds ballot into the PCOS machine	<p>The SAES-1800 is inherently not transparent particularly because there is no sufficient mechanism for verifiability of voter’s choice. The voter will not know if his/her ballot will be counted and how by the machine because once the ballot is fed into the machine, then it is up to the system to count the votes invisibly to the public. This is in violation of Article 7 (n) of RA 9369 which states that the automated election technology should “Provide the voter a system of verification to find out whether or not the machine has registered his choice.”</p> <p>Aside from this problem, these possible scenarios can arise:</p> <ul style="list-style-type: none"> <li>- Pre-marked legitimate ballots might be fed</li> <li>- Legitimate ballots rejected (putting a mark on the security markings will make the machine reject the ballot)</li> <li>- Reading/scanning ballots from another precinct</li> <li>- Hardware/software failure</li> <li>- No backup units arrive</li> </ul>	<p>To comply with this provision of the law, the Comelec must enable the feature of the SAES-1800 that will show how the PCOS machine interpreted the ballot.</p> <p>The way that the PCOS machine interpreted the voter’s ballot must be part of the audit trail attached to the ballot image (TIFF file) in addition to what is provided for in the RFP/TOR. This can be put in after a review of the source code is conducted.</p>
19	Election day	BEIs close polls	<p>These possible scenarios can arise at this stage on election day:</p> <ul style="list-style-type: none"> <li>- Failure of function to close polls</li> </ul>	<p>A system of verifiability of voter’s choice should be implemented as well as the review of the source code.</p>

			<ul style="list-style-type: none"> <li>- Misreading of ballots</li> <li>- Mis-crediting of marks</li> <li>- Erroneous counting</li> </ul> <p>The first scenario happened in many incidents during the ARMM 2008 election; this can lead to the feeding of pre-marked ballots that can still be tallied.</p> <p>The last three scenarios (misreading of ballots, mis-crediting of marks, and erroneous counting) can occur in the absence of a source code review as well as a system of verifiability of voter's choice.</p>	<p>Comelec should also put in place a continuity plan on how to address the possible problem of failure of function to close polls.</p> <p>Poll watchers and political parties should make sure that as soon as the voting day ended that no ballots should be fed into the machine anymore.</p>
20	Election day	BEIs generate and print ER	<p>Party List groups do not receive a copy of ERs despite 30 sets already provided by the law.</p> <p>Aside from this there can be hardware or software failure wherein the printer fails, no back up units arrive, or there is a failure of function to generate and print ER.</p> <p>The law states that the "Election returns transmitted electronically and digitally signed shall be considered as official election results and shall be used as the basis for the canvassing of votes and the proclamation of a candidate" (Sec. 19 (13)).</p> <p>This means that the printed ER will not have any use in forming the basis of the proclamation of a candidate. In essence the printed ER will not have any bearing on the outcome of the elections even if the printed ER differs with that of the electronically-transmitted ER received by the canvassing centers.</p>	<p>Poll watchers and political parties must cross check the printed ER with the one that will be digitally signed and transmitted by the BEIs to canvassing centers. The two should be the same. This however is not a guarantee that the checked ER will be canvassed (see Vulnerability #22 and #27 below).</p>
21	Election day	Formulation of the Election Return Certification Statement	<p>Without a verification system, the certification on the printed Election Return demonstrated by Smartmatic that</p>	<p>In the absence of a verification system, Comelec should re-word the Certification statement on the</p>

			<p>states “We hereby certify that we witnessed the voting at the precinct and that the votes obtained by each candidate appearing in this election report are <b>true</b> as generated by the Precinct-Count Optical Scan (PCOS) machine” may cause confusion among the BEIs and poll watchers. In the absence of verifiability of voter’s choice and public counting, BEIs might refuse to sign the said certification statement that includes the word “true.” This was indicated to the study team by a group of teachers who will serve as BEIs in 2010.</p>	<p>Election Return. But more than this, it should enable the feature in the SAES-1800 that will provide a system of verifiability of voter’s choice.</p>
22	Election day	BEIs digitally sign and encrypt the electronic ER using their digital signatures	<p>The digital signature on the precinct ER is a summary (hash value) of the ER encrypted using the BEI’s secret key. The digital signature serves two purposes: (1) it identifies the BEI personnel and the precinct number from which the ER came; and (2) it ensures that the precinct ER is not modified in any way by <i>dagdag-bawas</i> (immutability of precinct data).</p> <p>Because of its importance in maintaining data integrity and security, the secret key of the BEI which will be used to digitally sign and encrypt the ER to prevent <i>dagdag-bawas</i> is of utmost importance.</p> <p>However Comelec Bid Bulletin No. 10 27 April 2009 Public Bidding / 2010 Elections Automation Project promulgated on 15 April 2009 states:</p> <p>“The digital signature shall be assigned by the winning bidder to all members of the BEI and the BOC (whether city, municipal, provincial, district). For the NBOCs, the digital signatures shall be assigned to all members of the Commission and to the Senate President and the House Speaker.</p>	<p>Comelec should have a plan to ensure that the secret key of the teacher should be known only by the teacher and enough security should be put into place to ensure that the secret key is not divulged to Smartmatic-TIM, Comelec or to the PCOS machine during the certificate application step and the digital signing step. Furthermore, the ER and digital signature (encrypted hash value) should never be separated during transmission and storage in the Comelec databases.</p>

			<p>The digital signature shall be issued by a certificate authority nominated by the winning bidder and approved by the Comelec.”</p> <p>If this happens, if Smartmatic gets a copy of the secret keys of the BEIs, it would theoretically have the power to change the ERs.</p>	
23	Election day	BEIs digitally-transmit the digitally-signed ER to the canvassing centers (Municipal/city, Provincial, Congress, and Comelec)	<p>Transmission failure and connectivity failure can arise at this stage in the voting day if the transmission infrastructure is inadequate or made inoperable. At the same time, denial of service attack or transmission sites being physically attacked to cut off signal in a particular area are also possible scenarios.</p> <p>If the BEIs cannot digitally transmit the ER, they will have to physically bring the electronic ER contained in a removable device to the municipal or city canvassing centers. This can expose the BEIs to harassment, the same problem they faced in the manual elections.</p>	<p>Comelec should be clear regarding the realistic condition of transmission infrastructures in the country. It should have also come up with a Geographic Information System (GIS) mapping and analysis of various infrastructures such as telecommunication, road and power infrastructures, and satellite systems before it came out with the adoption of the PCOS technology for the 2010 elections. The GIS is important in ascertaining the feasibility of the chosen technology to deliver clean, credible, and transparent elections in 2010.</p> <p>Comelec should have a viable continuity plan should this scenario happen.</p>
24	Election day	<p>BEI creates a back-up copy of the following files to a removable data storage device, which shall be finalized and closed from further Write operations:</p> <ol style="list-style-type: none"> <li>1. Digitally signed and encrypted precinct results;</li> <li>2. Print file of the ER;</li> <li>3. Precinct’s statistical report;</li> <li>4. PCOS unit’s audit log report;</li> </ol> <p>and</p>	<p>RA 9369 gives conflicting statements regarding the official ER. Sec 19 (13) states that the official ER is the electronically transmitted digitally signed ER. However, a succeeding paragraph in the same section states that the digitally signed electronically transmitted ER <b>or</b> the ER stored in a removable device are the official ERs. In the event that both ERs do not match, which will serve as the official ER?</p> <p>If the transmission fails, this same section can mean that the BEIs can physically bring the back-up copy of the ER to the canvassing centers which happened during the ARMM 2008 elections. With cheating machineries still</p>	<p>Comelec should clarify what is stated in the law and immediately come up with an IRR.</p> <p>Comelec should also require that ballot interpretation attached to the ballot image should also be included in the back-up copy. This feature can be addressed if the source code is reviewed.</p> <p>Watchers and political parties should be allowed to have a copy of the back-up files so they can conduct their own tally based on the image and machine interpretation of the ballots actually cast. With this evidence, the electronically transmitted ERs</p>

		5. Digitally signed and encrypted voted ballot images.	<p>intact, this can expose the BEIs to harassment and the ER data to tampering.</p> <p>Moreover, the data prescribed to be stored does not indicate a requirement to store how the PCOS machine interpreted the ballot. If only ballot images are stored, the BEIs and watchers will never know how these ballot images were interpreted and if this interpretation is the one reflected in the ER.</p>	received by canvassing centers can be further double-checked for immutability.
25	Election day	BOC starts canvassing computers	Hardware or software failure can occur at this stage in the canvassing.	Comelec should have a viable continuity plan should this scenario happen.
26	Election day	BOC computers electronically accumulate the ERs into SOVs and COCs	<p>Possible problems include:</p> <ul style="list-style-type: none"> <li>- Transmission failure</li> <li>- Hardware and software failure</li> </ul>	Comelec should have a viable continuity plan should this scenario happen.
27	Election day	Root User /Administrator of the Machines	The root user/system administrator or “super user” of any computer is a human who can issue any command available on the computer, normally to do system maintenance or to recover from failure. But the root user can also do steps to cheat during elections because of his power. The root user can edit the precinct ERs if s/he has access to secret keys and therefore change the election results during canvassing.	<p>Comelec should put into place enough precautions so that a root user is not needed to manually interfere with the election programs or in case of a breakdown, the root user’s activities are all properly logged in publicly displayed audit and log files in real time to be scrutinized by poll watchers. Furthermore, the root user/s should never be allowed to log in from any remote location.</p> <p>IT-competent poll watchers should be deployed in canvassing centers where the root user/s are located. All of the actions of the root user/s must be scrutinized. The audit log should not contain any activities that would indicate a revision of the log files or of transmitted ERs.</p>
28	Election day	BOC generates and prints SOV and COC	<p>Possible problems include:</p> <ul style="list-style-type: none"> <li>- Printer failure</li> </ul>	Comelec should have a viable continuity plan should this scenario happen.

29	Election day	BOC digitally signs SOV and COC before electronically transmitting it to the provincial and national canvassing centers	As with the case of the secret keys of the BEIs, the secret keys of the BOC should also be safeguarded by the BOC against possible theft or copying. This is the only way that the immutability of the SOV and COC is ensured.	Comelec should have a plan to ensure that the secret key of the BOC should be known only by the BOC and enough security should be put in place to ensure that the secret key is not divulged to Smartmatic-TIM, Comelec or to the canvassing machine during the certificate application step and the digital signing step. Furthermore, the SOV and COC and digital signature (encrypted hash value of the ER) should never be separated during transmission and storage in the Comelec databases.
30		In 2-3 days, the winners are known and proclaimed	The process of adjudication in an automated election is either none or vague; likewise, there is little or no time to lodge electoral protests. It is a realistic scenario that losing candidates will not accept defeat especially if their watchers did not see how the ballots were interpreted, counted, and tallied by the PCOS machine.	Comelec should immediately come out with rules of procedures for election <u>adjudication</u> in an automated election: how to lodge electoral protests, what are the rules and mechanisms for resolving legal issues during elections, etc

\*About the 30+ Vulnerabilities of the AES 2010 (originally titled 30+ Vulnerable Spots)

Initially organized and drafted by Evita Jimenez, CenPEG, April 14, 2009

Revised and developed by Rosa Cordillera Castillo with inputs from Elsa Gines, Unyx Sta. Ana, Pablo Manalastas and Edwin Tuazon

& the AES Policy Study Team-UP College of Law (Office of the Dean)

CenPEG 2010 [www.cenpeg.org](http://www.cenpeg.org)

For further inquiries, Telefax 9299526 and email: [cenpeg.info@gmail.com](mailto:cenpeg.info@gmail.com)