



PRESS RELEASE

NEWS RELEASE

Center for People Empowerment in Governance (CenPEG)

July 6, 2009

THINK TANK BARES 30+ VULNERABLE SPOTS OF AUTOMATED POLL 2010

Unless Comelec and the consortium Smartmatic-TIM install safeguards and security measures to their automated election system (AES) soon, the country may end up with an automated disaster in May 2010.

The Center for People Empowerment in Governance (CenPEG) today revealed that it has identified at least 30+ vulnerable spots in the AES, and the list is growing. The list is part of the UP-based think tank's ongoing study on the AES in partnership with the UP College of Law.

The vulnerable spots, Prof. Bobby Tuazon, CenPEG's political analyst said, are in place in the whole system from ballot printing, warehousing of the counting machines to hardware and software deficiencies, voting, counting, electronic transmission of votes to canvassing and proclamation of winners.

The alarming list, he said, does not include weak spots in the infrastructure system such as telecommunications, phone and electric lines, and cell sites.

Aside from this, the fact alone that the automated election has been recently wracked by a tiff between Smartmatic and TIM reportedly over money and Comelec's failure to verify the winning bidder's key incorporation documents and "political neutrality" as its own rule requires makes the automated election off to a tainted start, Tuazon said.

Some of the vulnerable spots are the lack of a source code review, possible lapses in the digital signature, possible unofficial access to the canvassing servers, and the lack of voter's verifiability.

Center for People Empowerment in Governance (CenPEG)

3/F, College of Social Work and Community Development Bldg., University of the Philippines, Diliman, Quezon City, Philippines
Telefax: +632-9299526 email: cenpeg@cenpeg.org; cenpeg.info@gmail.com website: <http://www.cenpeg.org>



PRESS RELEASE

The review of the source code by independent ICT experts and other “interested parties”, which the election modernization law (RA 9369) requires, can verify whether the counting and canvassing are done properly and no cheating is possible. The review was not done in the August 2008 ARMM elections – and the Comelec has yet to respond to CenPEG’s official request last May 26 to provide the source code for review.

“The 30+ vulnerable spots should even prompt the PNP to revise its list of six ‘election hot spots’,” Tuazon said. “The system’s vulnerabilities make the whole AES fragile and prone to internal rigging, tampering, retail and wholesale cheating all over the country. The infrastructure system may even be vulnerable to jamming, sabotage, and other threats by some groups with the intent to cause a failure of election or manipulate election returns.”

“Election hot spots” should not begin and end with the incidence of violence, Tuazon said. “In the 2010 automated poll, the whole country is an election hot spot,” he said.

CenPEG’s political analyst also asked the Comelec “to stop spreading the illusion that with technology everything is A-OK and for Smartmatic-TIM to refrain from hyping about a ‘dream poll’ because both claims are unfounded.”

With the way Comelec appears to be cutting corners and changing its calendar many times in its haste to automate the elections there is now uncertainty whether the poll body may even install safeguards and security measures in the whole AES system, he said.

“At the very least, millions of voters could be disenfranchised thus damaging even more the country’s electoral process,” he said.

CenPEG is an independent policy institute based in UP Diliman, Quezon City. It is an official observer in Comelec’s procurement and bid process as well as of the Senate committee on constitutional amendments. Its studies about the AES are available for downloading at www.cenpeg.org.

For details of this news release, please contact:

Ms. Roda Manalac
CenPEG Tel/Fax 9299526
Mobile Phone No. 0929 8007965
Email: cenpeg.info@gmail.com