



# COMELEC "ALLOWS" SOURCE CODE REVIEW: A COMMENTARY

**Pablo Manalastas, PhD**  
Fellow and IT Consultant, CenPEG  
Faculty, Ateneo and UP computer studies

COMELEC has announced recently that it will allow source code review of the Election 2010 computer programs under closed and secure conditions. It also issued the following guidelines for programmers of interested political parties and groups who want to do the review.

1. Entities interested in conducting a source code review must signify their interest in writing for approval of the COMELEC and submit to COMELEC the credentials of their source code reviewers.
2. Entities approved by COMELEC shall sign a non-disclosure agreement before they are allowed to conduct the source code review.
3. Entities which will conduct the source code review shall submit to COMELEC the methodologies they propose to use.
4. COMELEC shall provide a secure and enclosed location/facility for the conduct of the source code review; and all entries and exits into the facility shall be properly recorded.
5. A read-only copy of the source code shall be provided on secured COMELEC workstations in the secured location/facility.
6. No copies of the source code or any part thereof maybe taken out from the secured location/facility.
7. No electronic devices of any kind, including but not limited to laptops, mobile phones, cameras, USB drives and other storage devices, shall be permitted inside the secured location/facility.
8. Each entity that conducts a source code review shall submit a report to the COMELEC after the review period.
9. The COMELEC reserves the right to issue supplemental guidelines in the conduct of the source code review.

James Ott, security specialist of Systest Labs, stated that the PCOS program is written in C/C++, and the CCS-REIS program is written in Java with Ant build tool. So if you have done programming in any of the following languages C, C++, Java, and you are comfortable programming using a Linux box, then we need you to help with the source code review.



I have some very serious reservations about the source code review being allowed by COMELEC. Let me name some of these reservations.

**1. Source Code Review is a Right of the People, Not a Privilege Granted by COMELEC.** From the tone of the above-mentioned guidelines, one gets the impression that COMELEC is bending over to accommodate the source code review requests of interested political parties and groups, like the Center for People Empowerment in Governance (CenPEG). Also from the detailed enumeration of what the reviewers are not allowed to do, specially as affected by Guideline Nos. 4,5,6 and 7, COMELEC seems to be putting up all possible barriers to reviewers in order to make the review as difficult as possible. That source code review is a right of the people is subsumed in the right to information guaranteed by Section 7 in the Bill of Rights in our Constitution. Furthermore, Section 14 of the Automated Election System Law (RA-9369 AES-Revised) mandates COMELEC, among the very first steps in computerization of elections, to make the source code available and open to reviewers to conduct their own reviews, independent of COMELEC's review done by Systest Labs:

"Once an AES technology is selected for implementation, the Commission shall promptly make the source code of that technology available and open to any interested political party or groups which may conduct their own review thereof."

The lawyers of COMELEC, in various documents that they issued, have twisted the interpretation of this simple straightforward IT requirement, to force independent reviewers to conduct their review under terms and conditions dictated by COMELEC, in such place and in such duration that COMELEC, in its infinite wisdom, decide that independent reviewers deserve, which is less than 90 days before actual election date. I am requesting COMELEC to cite an example of a source code review of the computer programs for a national election of such scope as Philippine Election 2010 that turned out be trustworthy, reliable, and believable source code review. If ever, this COMELEC-controlled source code review will be the first in the world history of computing to end up being a big failure, because COMELEC did not give the reviewers a "fighting" chance.

Source code review consists of reading and studying the computer programs that will be used in Election 2010, namely the PCOS program and the CCS-REIS program, and when time permits, the Election Management System Utilities (EMS) that are used to create the ballot faces and the XML files for use by the PCOS program and the CCS-REIS program. The objective of the review is to check that these programs conform to Philippine election laws, like the Omnibus Election Code BP881, AES Law RA8436, AES Law Revised RA9369, COMELEC 2009 TOR/RFP, and the COMELEC 2010 General Instructions, and are properly written election programs as specified in US-EAC-2005-VVSG, where the provisions of 2005VVSG do not conflict with our local laws. Furthermore, we would like these programs to be written as secure programs, secure from within, and secure from external attacks. For example, we would like stack limit checking, buffer overflow handling, proper handling of shared memory access, proper handling of socket calls, and digital signing according to present-day standards. Reviewing the programs for these features takes time, time that COMELEC does not want to give to reviewers.



**2. COMELEC Might Not Have the License to Allow Source Code Review by Third Parties.** It is entirely possible that when a programmer of a political party or interested group joins in the source code review under COMELEC-controlled conditions, that the programmer might be participating in an illegal activity -- one that violates the intellectual property rights of the copyright owners, one of which is Dominion Voting Systems. This is because a reading of Item 6 of the binary-level Licensing Agreement between copyright owner Dominion Voting Systems (of Canada) and software licensee Smartmatic International provides that "... all software and firmware, including the Democracy Suite EMS and the Democracy Suite ImageCast PCOS are hereby licensed to Smartmatic with the right to sublicense the right to use such software to the Commission on Elections for the Republic of the Philippines (COMELEC)". The license does not give the COMELEC any right to allow review of the DOMINION source code by third parties; it only gives COMELEC the right to use the EMS and PCOS programs for Philippine elections. In fact Item 7 of the same Licensing Agreement implicitly prohibits Smartmatic (and therefore prohibits COMELEC) from amending, changing, or developing enhancements, which can only be done during a source code review. This prohibition is implicit in Item 7, which states that "Dominion will retain sole liability to amend, change or develop all software, or firmware or EMS".

There are two ways around this problem:

(a) COMELEC could apply directly with Dominion for the correct source-level license with the right to sublicense the source code to "any interested political party or groups which may conduct their own review thereof", as provided for by Section 14 of RA9369. If Dominion grants this license to COMELEC, then the independent reviewers will have the right to review to their hearts' content, and to do the reviews at the times and places of their own choosing. There is a good chance that Dominion might grant this license, considering that they have already given such license to New York State (NYS). In the July 16, 2009 issue of Business Wire, NYS Board of Elections Co-Chair Doug Kellner stated, "... I am also pleased that Dominion has made all of its source code available for review to the New York State Board of Elections and its Citizens' Election Modernization Advisory Committee ...". Obtaining the proper source-level license is the honorable solution to this problem.

(b) If COMELEC fails to secure source-level licensing from Dominion, then the least COMELEC should do is to sign a waiver that absolves all programmer-reviewers of any liability for participating in the illegal activity of source code review without proper license, and further to undertake it upon itself the responsibility for any such liability. I am not a lawyer, but I think this solution sucks, and may in fact "not hold water" before any court.

The root of this problem is COMELEC's failure to see this flaw in the Licensing Agreement between Dominion and Smartmatic. Compound this situation with the fact that the COMELEC Advisory Council, COMELEC's adviser on such technical matters, also did not see this flaw, when it is its duty to watch out for such flaws and to protect COMELEC from committing such errors.

The problem could have been avoided if the COMELEC required of all seven (or ten) bidders the submission of the source code and the proper source-level licensing, to be included among the bid documents. If the source code were a prerequisite to join the bidding, as is done as a matter of standard procedure in a number of states in the United States, then the source code review can even be done ahead of time, even before award of contract.



**3. Signing a Nondisclosure Agreement, and Reporting Review Results to the Public, Are Contradictory Purposes.** I want to join the source code review because, as a Filipino programmer, I want to know how the PCOS and CCS programs scan our ballots, assign votes to candidates, count, summarize, digitally sign, encrypt, transmit, consolidate, and canvass our votes. I also want to report to the public, the Filipino voters, my review findings, because it is their right to know. In the absence of public counting in a computerized election, the source code review reports of independent programmers not under control nor under the payroll of COMELEC should be more believable than any source code review done by Systest Labs.

Since I have to report my review findings to the people, I can not sign a nondisclosure agreement (Item 2 of the COMELEC Guidelines).

You can not compare the computer programs used by banks for their on-line transaction processing with the computer programs used for national and local elections. In the case of banking transactions, the secrecy of the computer source code is sacred, because if a hacker-thief learns of the vulnerabilities of the banking system from reviewing the source code, he could steal money from the depositors using his knowledge of the vulnerabilities. But the computer programs for elections are different. Just as you want to know how the teachers belonging to the Board of Election Inspectors are counting your votes in a manual election, and in fact you want to watch them count your votes in a manual election, you also want to know, and want to watch the computer count your votes in a computerized election. But the computer is too fast, so you can not see what it is doing. So you rely instead on the programmer-reviewers, who will watch what the program is doing, by reading the source code. So the reviewers will do the watching for you, and make sure that your votes are counted.

**To summarize:** Being a programmer, I want to join the source code review of the PCOS and CCS computer programs. I am willing to do my share of the review for free, gratis, even though I know that COMELEC paid Systest PHP70 million of our tax money to have them do a source code review and program testing. However, I am willing to work only if COMELEC gives a satisfactory resolution to the three reservations that I have enumerated here.