

September 28, 2010

HON. JOSE A.R. MELO
Chairman
Commission on Elections
Intramuros, Manila

Dear Chairman Melo:

This refers to the Comelec's May 8, 2010 compliance with the May 6, 2010 Resolution of the Supreme Court in SC G.R. No.191846, entitled "Guingona Jr., *et al.* v. Comelec," the dispositive portion of which reads:

WHEREFORE, we GRANT the petition in part. Respondent Commission on Elections is ORDERED, within two (2) days from receipt of this Resolution, to disclose to petitioners and the public the following:

1. The nature and security of all equipment and devices, including their hardware and software components, to be used in the 10 May 2010 automated elections, as provided for in Section 7 of Republic Act No. 9369;
2. The source code for review by interested parties as mandated by Section 12 of Republic Act No. 9369;
3. The terms and protocols of the random manual audit, as mandated by Section 24 of Republic Act No. 9369;
4. A certification from the Technical Evaluation Committee that the entire Automated Election System is fully functional and that a continuity plan is already in place, as mandated by Sections 9 and 11 of Republic Act No. 9369; and
5. The certification protocol and the actual certification issued by the Department of Science and Technology

that the 240,000 Board of Election Inspectors all over the country are trained to use the Automated Election System, as required by Section 3 of Republic Act No. 9369.

This Resolution is immediately executory.

As indicated in the cover letter signed by Executive Director Jose M. Tolentino Jr., the Comelec's compliance covered the submission of the following:

1. One (1) compact disc containing the nature of all equipment and devices, including their hardware and software components, to be used in the May 10, 2010 automated elections;
2. Copy of COMELEC Minute Resolution No.10-0138 dated February 10, 2010, on the Guidelines in the conduct of source code review of the Automated Election System for the May 10, 2010 National and Local Elections;
3. Copy of COMELEC Resolution No.8837 dated April 30, 2010, entitled "In the Matter of the General Instructions for the Conduct of a Random Manual Audit (RMA) for the May 10, 2010 National and Local Election";
4. Copy of Resolution No. 2010-002 dated 9 March 2010 of the Technical Evaluation Committee, entitled "Certification of the Automated Election System (AES) for the May 10, 2010 National and Local Elections", with Annexes; and
5. Copies of the Department of Science and Technology Certification Program Protocol and General Instructions, and the Memorandum dated May 7, 2010 of Ms. Carmelita M. Fortez, Human Resources Management Officer V, Personnel Department, regarding the number of the BEI members that were certified by the DOST.

Upon referral of said documents to the Information Technology experts from the Center of People Empowerment in Governance (CenPEG) for assistance we learned to our dismay that the documents forwarded to us were totally lacking in providing the information to the public as mandated by law and as

directed the Supreme Court necessary for a complete study of the Automated Election System (AES) used for the May 10, 2010 elections.

Furthermore, we were advised that the June 3, 2010 letter request of CenPEG for availment of twenty-one (21) documents were perfunctorily denied by the Comelec in its Regular *En Banc* meeting on July 6, 2010 without any reason given despite the fact that majority of the documents requested were covered by the items enumerated in May 6, 2010 Resolution, particularly the source code of all AES components and the documents on the nature and security of the equipment and devices, including the hardware and software of the AES system.

To emphasize the duty of the Comelec to release to the public the source code of the different components of the AES system, the Supreme Court *en banc* rendered its September 21, 2010 Decision in SC G.R. No. 189546, entitled "*CenPEG v. Comelec*" the dispositive portion of which reads:

WHEREFORE, the Court GRANTS the petition for *mandamus* and DIRECTS the COMELEC to make the source codes for the AES technologies it selected available for implementation pursuant to R.A. 9369 immediately available to CenPEG and all other interested political parties or groups for independent review.

Clearly, the Comelec is duty bound to fully disclose to the public all the documents necessary as provided for in the above-mentioned Supreme Court decisions.

For sake of specificity, we seek the release of the following documents, to wit:

The nature and security of all equipment and devices, including their hardware and software components, to be used in the 10 May 2010 automated elections, as provided for in Section 7 of Republic Act No. 9369.

Sec. 7 of RA 9369 refers to the Minimum Systems Capabilities of the AES which provided among others -

- (a) adequate security against unauthorized access;

(b) accuracy in recording and reading of votes as well as in the tabulation, consolidation/canvassing, electronic transmission and storage of results.

xxx

(g) an election management system for preparing ballots and programs for use in the casting and counting of votes and to consolidate, report and display election results in the shortest time possible;

xxx

The documents in the CD forwarded to us contain the following:

1. Election Management System (EMS) Security Specification
2. Consolidated/Canvassing System (CCS) Security Specification
3. Precinct Counting Optical Scan (PCOS) System Requirements Specifications
4. Precinct Counting Optical Scan (PCOS) Functionality Description and Operations Procedures

Although these documents give us a general idea of the security features of the EMS, CCS, and PCOS, these do not give enough details for a technical person to fully understand the security protocol involved.

In order to have a full and transparent review of the security features adopted, the Comelec should release to the public the following documents, to wit:

1. Public keys used by all PCOS & CCS-REIS computers and sample digitally signed documents, eg., Election Returns and Certificates of Canvass.
2. User manual of the PCOS, CCS-REIS & EMS computers
3. Encryption and decryption algorithms used by all PCOS and CCS-REIS computers during transmission
4. The network topology diagram and documentation
5. Hash code process documentation, specifically, the programs used for generating the hash codes of all programs used
6. Digital signing protocol used
7. Smartmatic-Comelec contract with complete annexes, including the security specifications

All of these documents are essential for the public -- including all citizens' groups and other interested political parties-- to properly review the nature and security-- of all AES equipment and devices, including their hardware and software components, used in the 10 May 2010 automated elections if the same performed properly, securely and accurately. The source code for review by interested parties as mandated by Section 12 of Republic Act No. 9369.

As compliance with this directive, Comelec simply forwarded Comelec Minute Resolution No. 10-0138 dated February 10, 210 providing the guidelines for the source code review under a controlled environment, specifically, to wit:

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.

These stringent conditions imposed are tantamount to a denial of the public's right to review the source code. We do not see the rationale or security risk behind these conditions especially when the request for the source codes review is being now sought after the May 10, 2010 elections.

In fact, the imposition of said conditions for the review of the source code under a controlled environment would run counter to the Supreme Court's directive in both of the above-mentioned cases cited for full public disclosure of the source codes. Said directive is without any qualification and unequivocal.

Accordingly, Comelec should release to the public the source code for the different components of the AES, to wit:

1. Source code of the PCOS & CCS-REIS programs
2. Source code of the encryption and decryption programs used in the PCOS and CCS-REIS programs
3. Source code of the digital signing program used in the PCOS and CCS-REIS computers
4. Source code of the modem
5. File formats of all data files used or produced by the PCOS & CCS-REIS programs and by the EMS
6. Customization report on the source code
7. Contract between Smartmatic and Dominion Voting Systems

A certification from the Technical Evaluation Committee that the entire Automated Election System is fully functional and that a continuity plan is already in place, as mandated by Sections 9 and 11 of Republic Act No. 9369.

Lastly, with regard to the copy of Resolution No. 2010-02 dated March 9, 2010 of the Technical Evaluation Committee forwarded to us, we note that the

same is an abridged version of the full report and we would like to secure a copy of the full report.

The above listed documents are necessary for a complete study of the AES. Without these documents there is no possible way for the public to ascertain with certainty the success of the AES during the May 10, 2010 elections amidst mounting doubts. The possibility of the same AES being utilized for the next national and local elections in 2013 gives us all the more reason for independent groups to validate the AES' success in performing properly, securely and accurately.

In the light of the above-mentioned Supreme Court decisions, we strongly urge you to release the above-mentioned documents to us and to all interested groups within five (5) days from receipt of this letter, otherwise, we shall be constrained to return to the Supreme Court and seek the appropriate legal remedies to compel the Comelec's full compliance with the decisions of the Supreme Court.

Thank you.

Very truly yours,



TEOFISTO C. GUINGONA JR.



BIENVENIDO LUMBERA

CHAIR, CENTER FOR PEOPLE EMPOWERMENT IN GOVERNANCE (CENPEG)