August 27, 2009

Shri Navin Chawla
Chief Election Commissioner
Election Commission of India
Nirvachan Sadan
New Delhi 110 001

Dear Sir,

This letter has response to your invitation apropos letter No. 51/8/16/9/2009-EMS (Vol.-VII) dated 22 August from the Election Commission (received by Email on 24th August) to make a demonstration in the Election Commission on the tamperability of ECI-Electronic Voting Machines (ECI-EVM's).

We hereby accept your invitation. As you would recall from our meeting with you on 17th August, 2009 at your office, we had agreed to begin the process of demonstration of the vulnerabilities & tamperability of Electronic Voting Machines upon receiving the intimation of a suitable date from ECI.

In the meeting referred above, we, the petitioners along with the team of Technical Experts from Netindia have outlined the process of tampering that we propose to adopt, with which the ECI representatives have concurred. In this regard, you may please refer to the proceedings of the meeting prepared by us enclosed with this letter (**Refer Annexure 1**). The Commission has also video recorded the entire proceedings of the meetings, which may be referred to.

As stated at the meeting, the broad outline and details of the tampering process to be adopted by our technical team to tamper with the EVM's is as follows:

1) What constitutes tampering of the EVM's will be spelled out and agreed to at the beginning of the process of tampering.

2) Steps & procedures in demonstrating the vulnerabilities of the present EVMs will be drawn in advance.

3) Our technical team will carry different tools--both hardware as well as software--related to reverse engineering for the purpose of the demonstration and the same shall be allowed by ECI. The ECI representatives accepted the same at the said meeting.

4) The process of tampering will take a few days and the time required to complete the process will be informed to the ECI after examining and inspecting the EVM's which may take a couple of days and will be carried out on 4th and 5th September.

Enclosed please find "Suggested Procedure for demonstration of the tamperability of the Electronic Voting Machines of ECI" **(Refer Annexure 2)**

As discussed in the meeting on August 17, we are submitting herewith a list of questions on the process, Expert Committee Report, Security and Technical aspects of EVM's. We shall appreciate receiving a response to all these questions before beginning the process of vulnerability demonstration. (**Refer Annexure 3)**

While the ECI has given us an opportunity to demonstrate the tamperability of the EVMs, this process is being scuttled by the Electronics Corporation of India (ECIL), one of the two public sector units manufacturing ECI-EVM's by serving a legal notice on all the the petitioners in the Hon'ble Supreme Court threatening all the petitioners with legal action. We are enclosing a copy of the same for your kind perusal. **(Refer Annexure 4)**

It appears to be too much of a coincidence that the ECIL legal notice was served on the petitioners just a day after we received the invitation from the Election Commission to demonstrate the tamperability of the ECI-EVM's on September 3. Is the ECIL's legal notice a deliberate attempt to prevent the petitioners of the PIL in the Supreme Court from exposing the tamperability of the EVM's?

We would like to respectfully submit to the Election Commission, a constitutional body, that these arm twisting attempts resorted to by one of your EVM suppliers (the ECIL) is not only an attempt to interfere with the process initiated by the Election Commission of India in deference to the order of the Hon'ble Supreme Court by giving us an opportunity to demonstrate the tamperability of ECI-EVM's, but is also in contempt of Hon'ble Supreme Court Orders.

We would like to urge the Election Commission, on whose behalf the EVM's are manufactured by the ECIL, to immediately give directions to the Public Sector Unit to withdraw their legal notice against our petitioners. If the Election Commission India fails to give such directions, we would be constrained to interpret that the ECIL, which is acting in contravention of the orders of the Hon'ble Supreme Court, has acted maliciously against the petitioners with the express knowledge of the Election Commission of India.

We look forward to discuss and finalise all the details regarding the vulnerability demonstration of the ECI-EVM's in the proposed meeting on 3rd September and commence the operations immediately thereafter.

Yours faithfully,

[V. V. RAO]
Petitioner in WP (c) 292/2009
Email: rtiap2005@gmail.com
Mob: 09849064309
HIG-155, Phase-V,
KPHB Colony, KKP,
Hyderabad (AP) 500072

Annexure 2

Suggested Procedure for demonstration of the tamperability of the Electronic Voting Machines of ECI

For the proposed reverse engineering of the ECI-EVM's to demonstrate their tamperability, finalizing the protocols is a prerequisite. The suggested procedure for demonstrating the tamperability of ECI-EVM';s is as follows:

Element 1: Finalisation of Verification Protocols

Initially, ECI and their technical committee shall demonstrate the complete operational process of the Electronic Voting Machines including the functional testing & security check methodologies adopted by ECI to test & certify the Electronic Voting machine that are currently in routine practice. And the same procedures shall be adopted by ECI to check & inspect the Electronic Voting Machines that the Petitioners & technical expert team post demonstration of tamperability of EVMs.

Element 2: Selection of EVM's of different models and makes

Our team would like to pick around 20EVMs from different locations carrying samples of various models developed (EVM w/o Dynamic key coding, New EVM with date & time stamp, EVM with Detachable Memory Module).

Element 3: Selection of EVM's for Tampering & Detection

As requested by ECI & accepted by the petitioners, technical experts from Netindia shall tamper a couple of EVMs and put them back into the 20EVM lot provided by ECI.

The tampered EVMs shall be kept for inspection to be checked & identified by people from these different categories:

1. Common Voter/Polling agent/Counting agent/Contestant
2. Election officials/ Presiding Officers
3. Technical Committee/ Manufacturer

The Technical committee/manufacturers shall adopt the same test process demonstrated at the beginning i.e. the same process of testing as in vogue currently, to identify the tampered machines.

Element 4: Team Size, Equipment and Risks involved

Petitioners shall deploy four or more engineers for the purpose and the ECI shall provide 24x7 access to the premises allocated for the purpose of tampering. Technical team shall be permitted to Open the boxes and test them to the component level. In the process, some circuit cards inside may get damaged or dismantled during reverse engineering.

By inviting the petitioners to demonstrate tamperability through the process of reverse engineering, it is construed and tacitly agreed by the ECI and the manufacturers that normal damage usually associated with such reverse engineering operations has been permitted by them.

A set of chips, PCBs and certain electronic components and any other tool as when required for the purpose of tampering the electronic voting machine relevant to the operation shall be allowed to be

carried in and out time of the ECI premises during the process. Wherever required, the technical team shall duly inform ECI with the details of the equipment & tools brought along with them into the premises. The list of equipment and tools, inclusive of but not limited to, that shall be carried by the technical team are as follows:

- Oscilloscope
- Logic Analyzer
- Micro grabbers - Probes
- Micro Controller boards
- Micro Chips
- Universal serial interface.
- Any other tool if required shall be intimated to ECI

Element 5: Stages of Tamperability Demonstration

The entire process shall be divided into IV Phases:

1. Demonstration of complete operational procedure of Electronic Voting Machines by ECI along with checks and balances adopted by ECI in routine Practice, Functional testing etc., as mentioned above.

2. Petitioner's technical team shall analyze the EVM boards for security lapses and Vulnerability Check and estimating the total time schedule for the Process. And shall intimate the time for the entire process of demonstration of vulnerability of electronic voting machine.

3. Reverse engineering and exploiting Vulnerabilities in EVM & Tampering a couple of EVMs out of the 20 EVMs.

4. Inspection and Identification by people from three different sectors and recording their observations separately.

Element 6: Independent Audit

As both the petitioners and the ECI are interested parties in the proposed exercise, as discussed in the 17th August meeting, a third party team of technical experts shall be jointly selected to validate the process adopted by both the parties. In addition, eminent personalities may also be selected to function as observers of the whole Proceedings.

ANNEXURE 3

List of questions submitted on Process;

Expert Committee Report & Security

This is the first set up questions for which written answers are requested as agreed in the meeting held at the Election Commission of India on 17th August, 2009 between the Election Commission representatives and the representatives of the writ petition in the Supreme Court.

After receiving the same, we would like to seek any further clarification that may be required.

Questions – On Process

1. What is the reason of using a generic chip instead of specifically designed ASIC chip in Electronic Voting Machine?
2. Is the Chip with same part number available in the market for others for developing other applications?
3. What is process involved in the procurement of the chip & who are the people involved in that process?
4. What is the precise transport process of sending the code to the chip vendor?
5. Does the Election commission have the information on procurement chips & the process involved?
6. Does Election Commission keep any audit/maintain a record on chips procured and chips used in EVMs, Chips damaged before manufacturing and chips in stock? Please provide the audit details from 1990 till date.
7. Is there any encryption in the Ballot unit used for transfer of the data to control unit, if so what is the encryption and what is the software used in the Ballot Unit for enabling such encryption?
8. Have the old machines been replaced, and how many more old machines have been used and can we obtain the manufacturing dates, batch numbers, serial numbers including the life of each of the Electronic Voting Machine used in the recent elections held? What is the status of the old mother boards in the upgraded machines?
9. Who are people involved in maintenance of EVM, are they permanent employees of ECIL / BEL or are there any contract labor involved? Please provide the details of the people.
10. In the recently concluded Elections, how many of the machines failed to read the E2PROM, & in case of memory becoming unreadable, what are the alternate methods adopted?
11. What does Election Commission do with the faulty machines, if they are repaired what is the process and who are the people / organizations involved, is there any Annual Maintenance Contract for the Electronic Voting Machines?
12. Is there any form of Randomization involved before EVM's are being sent to the Districts for the first level Randomization.
13. How many people are involved in the EVM code development? Have they signed any non disclosures on Code Security with ECI? Are all the developers are still working with

the ECIL/BEL? Is there any guarantee on code security formally provided by ECIL and BEL to ECI?

Questions – On Expert Committee Report

1. Was the Chip used an OTP (Where the code is fused in house at the manufacturer's location) or Masked ROM (Where the code is sent outside the country to be fused into the chip at the vendor's location)?
2. Are the CU & BU cards sealed and signed by the party representatives as suggested by the Prof. INDIRESAN committee report?
3. Is there a micro controller in the BU both in old and new machines? Is it the same OTP or mask as in CU or a different chip?
4. How many Electronic Voting Machines used were upgraded in the election held recently?
5. Is there a self test signature for every Electronic Voting Machine including machines prior to 2006 and post 2006? If there is a signature available what is the process adopted and what are the records maintained for the same?
6. Is there any other form of encryption used to store the data in EEPORM apart from dynamic key coding?
7. Is it a static allocation of memory in the EEPROM to store every vote like an incremental counter or whether it's read back vote by vote while results operation is being executed?
8. Did the Election Commission take the complete print out of every key pressed wherever there were incidents of Mal-Functioning of Electronic Voting Machines? As Expert Committee insisted on Data & Time Stamping every key pressed. Please provide details of such EVMs selected and the outcome after taking such printouts.
9. Why did Election Commission disregard certain suggestions made by the Expert Committee in regards with the modifications & upgrade of the Electronic Voting Machines used in the elections held recently?
10. What are the total number of votes that can be polled in an EVM, as Expert Review Report "Draft 1989-90 EVM's Replacement Additional features contemplated" mentions it to be 2000 maximum votes whereas FAQ's on ECI website mentioned it to be 3840? Is there a difference in the maximum votes between old & new machines?
11. What is the size of EEPROM used & what is the size of data used to store every vote?
12. What is the time diversity algorithm used for transmission of data? US Patent 4001692
13. Did Prof Indiresan committee evaluate the EVMs with detachable memory module (DMM)? If not why EVM-DMM models are not considered for evaluation? Are they used in any elections?
14. Had the technical committee led by Prof Indiresan considered the point on willful Trojans inserted by the developers themselves?
15. Can a simple functional test be able to identify a Trojan inserted?
16. What kind of verification process was involved in the evaluation of EVM's by Technical Committee i.e. UAT, Functional Test or a simple over all Process Check, further are there any reports of these tests available?
17. Post the changes made by the manufacturers of EVM according to the recommendations of Expert Committee review report were tests performed if so what are the test methods & test reports?

Questions – Security

1. What is the hardware level security (Board level & component level) on both the Ballot Unit & Control Unit provided to avoid Non-Invasive, Invasive & Semi-Invasive attacks?
2. Is there any security standard adopted in the EVM? If so please specify..
3. Are the EVMs covered or fall under E-Governance? Are e- governance standards applied to EVM?
4. What is the prevention mechanism against Replication of EVMs? Can it be identified by a non technical person?
5. Is there any test to validate the ballot unit other than the Mock poll? (As the mock poll is not possible in case of BU change in the middle of the poll).
6. How many EVM circuit cards are replaced on malfunction while maintenance? what is the status of the OLD cards?
7. How many machines are abducted/destroyed in poll disturbances? How many are recovered?
8. How many spare machines shall be kept ready per assembly constituency and parliament constituency? Are they part of First level and Second level randomization?
9. Who developed the Randomization software? Is there any kind of security validation done to the randomization software?

Questions – Technical

1. What are the specifications of Hardware, Firmware & Interfacing?
2. What are Standards & Guidelines followed while coding?
3. What are Standards followed for designing the Hardware?
4. What are the standards followed in designing the Encasings?
5. What are the Certifications available for Hardware?
6. What are the test cases & reports of the entire project?
7. Was any Risk Analysis performed?
8. What is methodology of Full Load test?
9. What are the fail safe parameters for Firmware, Hardware as well as Interfaces?
10. Was any Disaster recovery mechanism adopted?
11. Is the Hardware unit capable of interoperability, to avoid monopoly & vendor Lock-In?
12. What are the MTBF (Mean Time between Failures) of various components used?
13. Does the Program memory in the EVM chip is fully utilized by program? In case not is the space left out in the program memory is filled safe in the controller without Trojans?

Petitioner Technical Experts