मताधिकार फक्त लोकशाहीसाठी | VOTE FOR DEMOCRACY

April 16, 2025

Computer Science Experts question ECI's rebuttal of Tulsi Gabbard on Indian EVMs

Computer Science & Programming Experts who are part of Citizen's Collectives like Citizens Commission on Elections (CCE) and Vote for Democracy (VFD) have questioned the Election Commission of India (ECI)'s rebuttal of Tulsi Gabbard (Director of National Intelligence, US Gov)'s claim that Indian EVMs not connected to Internet, Wi-Fi, says Election Commission amid Tulsi Gabbard's comments - The Hindu

This Statement has been issued by Madhav Deshpande with 40 plus years of experience in the field of Computer Science and its Applications and Architecture of Unique Software apart from being a consultant to the Obama administration, Prof Harish Karnick, Retd. Prof. Dept. of Comp. Sc. and Engg., IIT, Kanpur, Kaushik Majumdar, Professor Indian Statistical Institute, Sarbendu Guha, Principal Product Engineer, Digital Infrastructure For India:

"We read with great concern this prompt statement by the Election Commission of India (ECI), Saturday, April 12 following Tulsi Gabbard, Tulsi Gabbard (Director of National Intelligence, US Government)'s claim on the vulnerability of the electronic voting system, the day before. At the outset we would like to state that it is shocking that the ECI responds so promptly to an official of a foreign government, even as it is obdurate and non-responsive to legitimate queries by Citizens, Experts and the Political Opposition."

This team of experts strongly disagrees with the ECI for the following reasons.

Manipulation of an Electronic Voting Machine (EVM) is the set of actions to make the EVM perform in the way it is not supposed to behave. Such manipulation can be effected by providing additional data to the Voter Verifiable Paper Audit Trail (VVPAT) using the Symbol Loading Unit (SLU). The SLU acquires its data when connected to the ECI website after the candidate list is finalized, which only a few days before the voting day.

While it is very difficult to alter the program instruction set in the one-time write locked EEPROM, it is entirely possible to:

a. Push a Trojan software through the USB drive when it is connected to the VVPAT for purpose of uploading the candidate list. Such Trojan software will modify the firmware as if the firmware is being "updated". The "updated" firmware will then perform manipulated malfunction to deliver manipulated results. It is important to note that ISP (In-System Programming) is an established way of updating the firmware of a microcontroller and as such is a ubiquitously accessible technique.

b. Supply additional data to the already burnt-in program. The program existing in the VVPAT must be already written to recognise the additional data and decision making branches already must exist in the program code to deliver manipulated functionality.

We also maintain that earlier version of EVMs used before 2014 Lok Sabha elections were intended to be stand-alone and therefore not open to manipulation. This earlier EVS system did not have the VVPAT unit nor the Symbol Loading Unit (SLU) and moreover, did not need data (mapping candidate/party symbol to buttons of the Ballot Unit-BU) nor any additional instruction set to be loaded into EVM-VVPAT through a physical communication port. Hence, the ECI's bald statement, without answering concerns by Indian Computer Science experts does not inspire confidence.

We are further concerned that the ECI has never demonstrated publicly and opened any operational CU, BU, and VVPAT in public presence. The ECI has never allowed any open door controlled testing of any working EVM in presence of Indian Public. It is not certified by any third party, neutral experts committee that the EVM does not emit or receive any Radio Frequency (RF) signal.

We demand that ECI should allow the Indian citizens to conduct non-invasive and non-destructive tests on the powered-on, working EVMs at 3 locations in every state to satisfy themselves that EVM does not respond to or create any RF communication channel. These EVMs must not be from the spare EVMs stored, but must be from those that were actually used in the 2024 Lok Sabha elections.

In addition, we demand that the ECI publishes the steps and processes followed to establish and prove data integrity across the entire Electronic Voting System or Electronic Election System.

We demand that the ECI publishes every step taken and the process at every step to establish and prove data integrity across the BU, CU (including the procedure to establish that both copies of electronic vote stored in the CU are identical), VVPAT (the data exchange between the VVPAT and the CU) and finally the values received by the counting unit (as applicable). The ECI must publish the detailed protocol it follows on the day of voting and the day of counting to establish that none of the above data has been changed.

The ECI's blanket statements that Indian EVMs are not connected to internet wirelessly /wired fashion (read external radio wave or microwave communication signals) without giving out details of the circuits is tantamount to official propaganda bereft of scientific or rational enquiry.

The problem is there are only claims (ECI) that the EVS is not connected but there is no proof demonstrated to the public. And without proof any claim is as good as a lie.

The Symbol-Loading Unit (SLU) of the VVPAT unit is connected to the ECI's website for a brief while - after the list of candidates and their symbols are finalized and before the date of polling. All details about the final list of candidates including their symbols are downloaded from the ECI's website on to the VVPAT unit.

There is an electronic security loophole here because it is possible to introduce a vote-stealing Trojan into the ECI's website, with or without the ECI's knowledge, and this Trojan can get downloaded into the VVPAT unit.

The vote-stealing Trojan can be so programmed as to get activated after a certain number of votes (say, 200 votes) have been cast, and to convert, say, every 5th vote cast thereafter to a vote for a certain political party, when the signal is transmitted from the VVPAT unit to the Control unit. The vote-stealing Trojan can also be programmed to self-destruct, say, 6 hours after the last vote has been cast, leaving no trace of its nefarious deed. The Trojan can be programmed to act only on a certain date and that too after a certain time of the day.

Further, the Trojan or the original program itself can be written to respond to additional data uploaded via SLU. Such program will display different behaviour in every constituency, based on the data uploaded from the SLU.

Therefore, we further demand that from each constituency, at least 3 randomly selected SLUs, (selected by public), should be given to open scrutiny by a committee of experts. This scrutiny should be carried out in full public view.

(Response of the CCE and VFD Experts)

On April 11, 2025 a group of over 80 Citizens including Experts had submitted a Detailed Memorandum to the Election Commission of India.

This can be read here: https://votefordemocracy.org.in/wp-content/uploads/2025/04/250411-Memorandum-ECI-MD-Modifications-for-website.pdf