Interim Report of the Citizens' Commission on Elections on EVMs and VVPAT

Executive Summary

January 16, 2021

Based on depositions by:

Poonam Agarwal, Journalist, The Quint. Deposition.

M G Devasahayam, IAS (Retired). Deposition.

Venkatesh Nayak, RTI Activist. Deposition.

Prasanna S, Advocate. Deposition.

Anupam Saraf, Professor and Future Designer. Deposition.

Subodh Sharma, Assistant Professor, Computer Science and Engineering, IIT Delhi. Deposition.

Sandeep Shukla, Professor, Computer Science and Engineering, IIT Kanpur. Deposition.

Bappa Sinha, Technologist, Free Software Movement of India. Deposition.

Poorvi L. Vora, Professor, Computer Science, George Washington University, Washington, DC, USA. Deposition. (joint submission)

Alok Choudhary, Professor, Electrical and Computer Engineering, Northwestern University, Evanston, Illinois, USA (joint submission with Poorvi Vora)

J. Alex Halderman, Professor, Computer Science and Engineering, University of Michigan, Ann Arbor, Michigan, USA (joint submission with Poorvi Vora)

Douglas W. Jones, Associate Professor, Computer Science, University of Iowa, Iowa City, Iowa, USA (joint submission with Poorvi Vora)

Nasir Memon, Professor, Computer Science and Engineering, New York University (Brooklyn), New York, New York, USA (joint submission with Poorvi Vora)

Bhagirath Narahari, Professor, Computer Science, George Washington University, Washington, DC, USA (joint submission with Poorvi Vora)

R. Ramanujam, Professor, Computer Science, Institute of Mathematical Sciences, Chennai, India (joint submission with Poorvi Vora)

Ronald L. Rivest, Professor, Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA (joint submission with Poorvi Vora)

Philip B. Stark, Professor of Statistics, University of California, Berkeley, USA (joint submission with Poorvi Vora)

K. V. Subrahmanyam, Professor, Computer Science, Chennai Mathematical Institute, Chennai, India (joint submission with Poorvi Vora)

Vanessa Teague, Associate Professor, School of Computing and Information Systems, University of Melbourne, Australia (joint submission with Poorvi Vora)

Depositions were also invited from the Election Commission of India and the members of its technical committee, Professors D. T. Shahani (IIT Delhi), Rajat Moona (IIT Bhilai) and D. K. Sharma (IIT Bombay). However, no deposition was received. The CCE also sent a questionnaire to the ECI, members of its technical committee and some former Chief Election Commissioners; only one response was received.

1 Democracy principles

The **democracy principles** that any voting process for public elections should adhere to are:

1. The voting process should be transparent in a manner that the general public can be satisfied that their vote is correctly recorded and counted.

2. The voting and counting process should be publicly auditable.

3. Ordinary citizens should be able to check the essential steps in the voting process. If special expert knowledge is required then all should be able to select their own experts.

4. There should be verifiability in the counting of votes and ascertainment of the results reliably without too much special knowledge.

5. An election process should not only be free and fair, but also be seen to be free and fair.

6. Election Commission should be in full control of the entire voting process, and the public at large should be able to verify.

7. Electronic processes, if they are to be used for voting, should be in sync with changing technologies and technological practices, and be subject to public scrutiny/examinability.

In this report we examine to what extent the Electronic Voting Machine (EVM) along with the Voter Verified Paper Audit Trail (VVPAT) based system used in India comply with the democratic principles and make some recommendations.

2 Concerns with the EVM

1. In an EVM, where votes are recorded electronically by press of a button, and the voter cannot examine what has been recorded, **there is no way to provide a guarantee to a voter** that her vote is *cast as intended* (recorded correctly in the EVM), *recorded as cast* (what is recorded in the EVM is what is collected in the final tally) and *counted as recorded*. This casts doubts on a purely EVM based system.

2. It is well known that theoretically establishing the correctness of a system as complicated as an EVM is a computationally intractable problem. It is also well known that Quality Assurance (QA) testing is never adequate to establish the correctness of an EVM, and such tests can detect only a small fraction of possible software or hardware errors (follows a common maxim that **tests do not constitute a proof of correctness**). Also, **pre-determined and preset test patterns are known to be inadequate for verification of the integrity of an EVM. The present EVM system is not verifiable and therefore is unfit for democratic elections**.

3. If the correctness of an EVM cannot be established then it is practically impossible to predict whether an EVM can be hacked or not. **In particular, that an EVM has not yet been detected to have been hacked provides no guarantee whatsoever that it cannot be hacked**. Thus **elections must be conducted assuming that the electronic voting machines may possibly be tampered with**.

4. Voter-verified Paper Audit Trail (VVPAT) is one possible to way to make the voting system auditable. Using VVPAT a voter can in principle verify that her vote is *cast as intended*, and a suitably designed end-of-poll statistical audit can possibly determine that the collection and counting are correct. This, however, is crucially dependent on the following three requirements:

   (a) That the VVPAT system is **truly voter-verified.** The correct VVPAT protocol is to allow a voter to approve the VVPAT slip before the vote is cast, and to provide an option to cancel her vote if a discrepancy is noticed. It also requires a clear protocol for dispute resolution if a voter complains that a VVPAT printout is incorrect.

   The ECI's VVPAT system is not truly voter-verified because it does not provide the necessary agency to a voter to cancel her vote if she thinks it has been recorded incorrectly. Also, in case the voter raises a dispute, there is no way for her to prove that she is not lying. As such, penalizing a voter in such a situation is not correct.

(b) There must be *compliance audit*, verifiable by all candidates and interested members of the general public, to ensure the integrity of the VVPAT slips. The VVPAT slips may be trustworthy at the time of voting, but it is necessary to ensure that they remain trustworthy later while auditing. Only then a subsequent statistical audit can establish the correctness of the voting process. There has to be sufficient guarantees against spurious injection or deletion of votes after polling and before counting when the EVMs and VVPATs are in custody of ECI, without requiring any trust assumptions. Otherwise, the mere agreement of electronic and VVPAT counts cannot rule out spurious vote injections or deletions in both.

(c) There must be post-election audit of the EVM counts against manual counting of the VVPAT slips. It is incorrect to assume that the prevalence of faulty (or hacked) EVMs is homogeneous across the population, independent of the margin of winning votes. In fact, it may be sufficient to tamper only a few EVMs to swing an election if a contest is close. Thus, in practice, it may be necessary to test more EVMs than even what the civil society and the political parties demand (30% and 50% respectively) to ensure verification and reliable ascertainment of results.

3 Recommendations

1. The decision making processes within the ECI need to be much more logical, rigorous and principled compared to what it was for the 2019 parliamentary elections.

2. **EVMs cannot be assumed to be tamper-proof**. The electronic voting system **should be redesigned to be software and hardware independent in order to be verifiable or auditable**. This does not imply that software or hardware cannot be used, but that the correctness of the election outcome cannot be entirely dependent on their working correctly.

3. The VVPAT system should be **re-designed to be fully voter-verified**. The voter should be able to approve the VVPAT printout before the vote is finally cast, and be able to cancel if there is an error.

4. The integrity of the VVPAT slips and the EVM machines during the entire time after polling and before counting and auditing must be ensured in a manner that is verifiable by all (and especially the candidates). There should be no trust requirement on the custody chain.

5. There must be stringent audit of the electronic vote count before the results are declared. The audit should not be based on ad hoc methods but by counting a statistically significant sample of the VVPAT slips according to rigorous and well established statistical audit techniques. The audit may in some cases - depending on the margin of victory - require a full manual counting of VVPAT slips.

6. There should be legislation to decide what is to be done if the audits reveal a problem. Such legislation should ideally be based on well established statistical procedures and not on subjective decision of a few officials.

7. There is a definite need to move away from certification of voting equipment and processes and demonstrate that the outcome of an election is correct irrespective of machines and trust on custody chains of EVMs. Two ways to do this are by adopting rigorous and well established strategies for **risk-limiting audits** or by using a **provably end-to-end verifiable cryptographic protocol**, or both. The **ECI should explore the possibilities**.

8. Finally, the voting system design should be subjected to independent (of the government and ECI) review and the integrity of the election process should be subjected to independent audit. **The findings should be made public**. In particular, all design details should be transparent and publicly available.