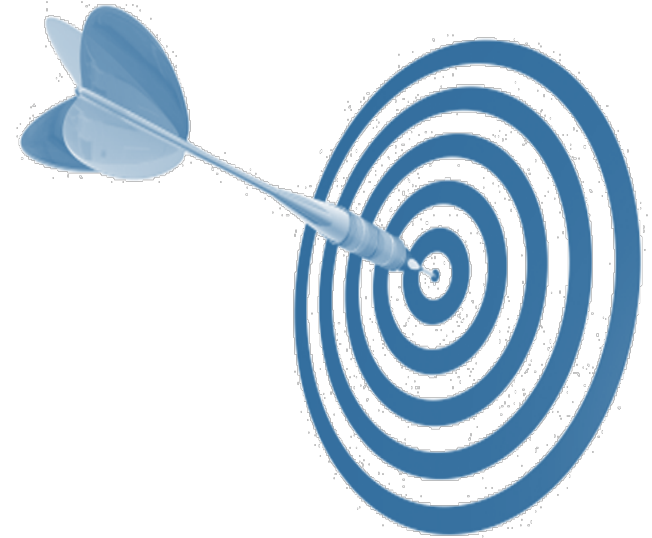




# PRESENTATION ON EVM & VVPAT

# AGENDA

1. History
2. Technical Expert Committee (TEC)
3. Technical Security
4. Administrative safeguards
5. Debate around EVMs- Explained
6. Aspersion Vs. Confidence
7. Past Judgements
8. VVPAT



# HISTORY OF EVM

40 YEARS

# HISTORY OF EVM – 40 YEARS



1977

CEC- S L Shakdar talked about introducing an Electronic machine

1980-81

EVMs developed and demonstrated by ECIL and BEL.

1982-83

EVMs used in 50 polling stations of Parur LA in Kerala.  
Used in 11 Assembly Constituencies: 8 states, 1UT

1984

Usage of EVMs suspended: SC ruling-EVMs had no legal sanctity

1988

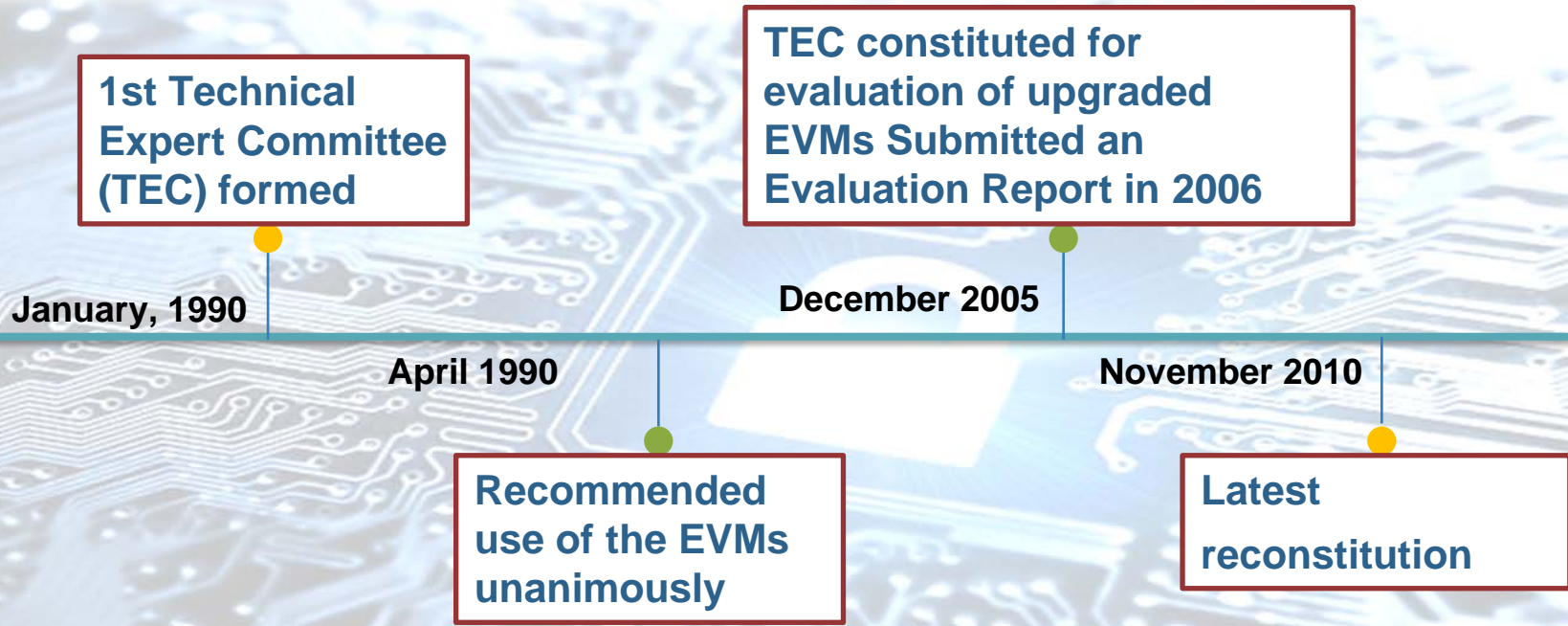
RP Act amended: allowing the use EVMs wef 15.03.1989

- **Since 2000, EVMs have been used in all elections. 3 Lok Sabha and 113 State Legislative Assemblies.**

# TECHNICAL EXPERT COMMITTEE

INDEPENDENT EVALUATION

# TEC- HISTORY & ROLE



# Past TECs

## **Composition of First Technical Expert Committee on EVMs – 1990**

1. Professor S. Sampath, Chairman Technical Advisory Committee, Defence Research & Development Organization (DRDO), Ministry of Defence
2. Professor P.V. Indiresan of the IIT Delhi
3. Dr. Rao C. Kasarabada, Director, Electronic Research & Development Centre (ERDC), Trivandrum

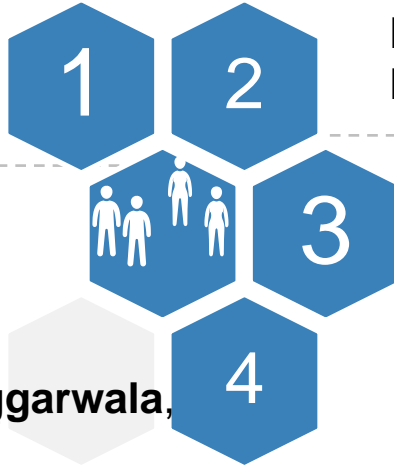
## **Composition of Second Technical Expert Committee – Dec 2005**

1. Prof P.V. Indiresan, Ex-Director, IIT Madras as Chairman of TEC
2. Prof. D.T. Shahani of IIT Delhi
3. Prof. A.K. Agarwala of IIT Delhi

# PRESENT TEC COMPOSITION

## 4 Eminent Professors from IITs: Renowned Experts in their Fields.

**Prof D T Shahani,**  
Prof Emeritus, IIT-  
Delhi.



**Prof Rajat Moona,**  
Director IIT Bhilai, Former  
Director General CDAC.

**Prof Dinesh K Sharma,**  
IIT Bombay

**Prof A K Aggarwala,**  
IIT Delhi

# ROLE OF TEC



Give technical advice to build specifications and design of newer versions of EVMs/VVPATs



Examine design proposals of manufacturers on EVMs and offer recommendations for improvement



Mentor design process, as well as R&D for further improvements in Evm & VVPATs



Supervising the Manufacturing process and the various QA & QC Test procedures and protocols by independent third party evaluators.



Examine concerns raised on EVMs tamperability

# TECHNICAL SECURITY

DESIGN, PROCESS, ENVIRONMENT



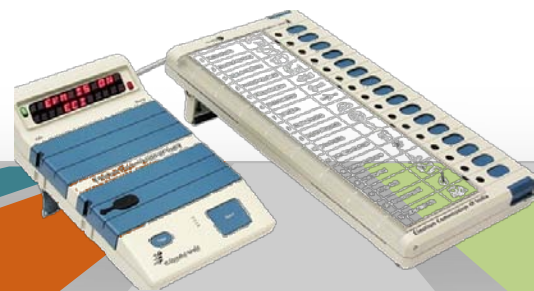
# 1. PREMIUM PSU MANUFACTURERS



Both PSUs deal with **manufacturing of sensitive equipment** critical to the safety and security of the Nation and have **strong security protocols**



## 2. SECURED DESIGN FEATURES



**Standalone  
Machine**


**No Radio  
Frequency  
transmission or  
reception  
possible- No  
wireless  
communication  
possible**

**One Time  
Programma  
ble (OTP)  
chip**



**Dynamic  
Coding  
of Key  
Press**

**Real Time Clock  
for time and date  
stamping key  
press**

### 3. SECURE DEVELOPMENT PROCESS



The software is designed/approved by TEC **NEVER subcontracted.**



Software validation is carried out as per the **System Requirement Specification (SRS)**, by an Independent Testing Group.



## 4. SECURE MANUFACTURING FACILITY

### Secure Factory Premises



- Monitored Entry and Exit
- Regular frisking at gates and all important junctions
- CCTV surveillance
- Entry of electronic gadgets like mobile, Laptop, USBs restricted

## 4. SECURE MANUFACTURING FACILITY



- Physical Security -CCTV surveillance and movement control
- Well defined and calibrated process flow of EVM manufacturing
- 3 Level Physical access to various stages / processes
- Access Data and Process Data logging, alarm and alert generation during manufacturing
- Third Party Testing by STQC as per Standards & Quality Process set by TEC



# EVOLUTION OF EVM MODELS

## ➤ Evolution of **technology**

## ➤ EVM Models

**Pre 2006: M1**

**2006-2010: M2**

**From 2013: M3**



- One Time Programmable Micro-Controller
- Standalone Machine



# EVOLUTION OF EVM MODELS



➤ Evolution of **technology**

➤ EVM Models

**Pre 2006: M1**

**2006-2010: M2**

**From 2013: M3**



- Dynamic coding of every key press for communication from BU to CU
- Real time clock
- Time stamping of key presses



# EVOLUTION OF EVM MODELS

- Evolution of **technology**
- EVM Models

**Pre 2006: M1**

**2006-2010: M2**

**From 2013: M3**



- Digital Certificate based mutual authentication amongst all components
- Automated Self Diagnostics
- Battery Life prediction



## SECURE MOVEMENT AFTER MANUFACTURING to the STATES/UTs



- **Any Movement of EVMs/VVPATs mandatorily tracked through ETS**
- **Only Containerized Trucks or Sealed trucks used for Transportation**
- **All Trucks sealed with Lock and Paper Seals**
- **GPS tracking**
- **All movement under 24X7 Police Escort**
- **Political parties informed in advance about the opening, stocking and sealing of warehouses while shifting of EVMs/VVPATs**
- **Videography done of shifting process**

# ADMINISTRATIVE SAFEGUARDS

SECURE HANDLING &  
MANAGEMENT OF  
EVMS/VVPATs



# ADMINISTRATIVE SAFEGUARDS ENSURE SECURE HANDLING AND MANAGEMENT OF EVMs AT ALL TIMES



1. Stakeholder Participation
2. Allocation & Movement
3. First Level Checking
4. Candidate Setting
5. Randomization
6. Mock Poll
7. Poll Day Checks
8. Poll Closure & Transportation
9. Storage & Security
10. Counting Day Protocol

# 1. STAKEHOLDER PARTICIPATION

## Active Participation of Political-Parties/Candidates in All Processes

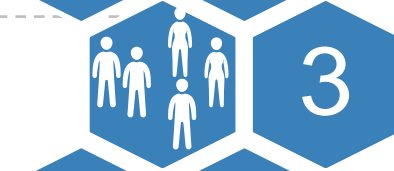
Opening & Sealing of EVM Warehouses & Strong-rooms.



First Level Check (FLC) & Candidate Setting.



Conduct mock poll and receive mock poll results



List of EVMs after first & second randomization



*Participation During FLC*



Sign on Paper Seals on BUs and CUs after all important processes

## 2. ALLOCATION & MOVEMENT

### Planned Allocation

EVMs are allocated to poll going State by the Commission

Received by DEO who is personally responsible for secured storage

EVM Tracking Software for inventory management of all EVMs nationwide.

### Secured Transportation



EVMs are always transported under 24/7 Police Escort irrespective of the destination

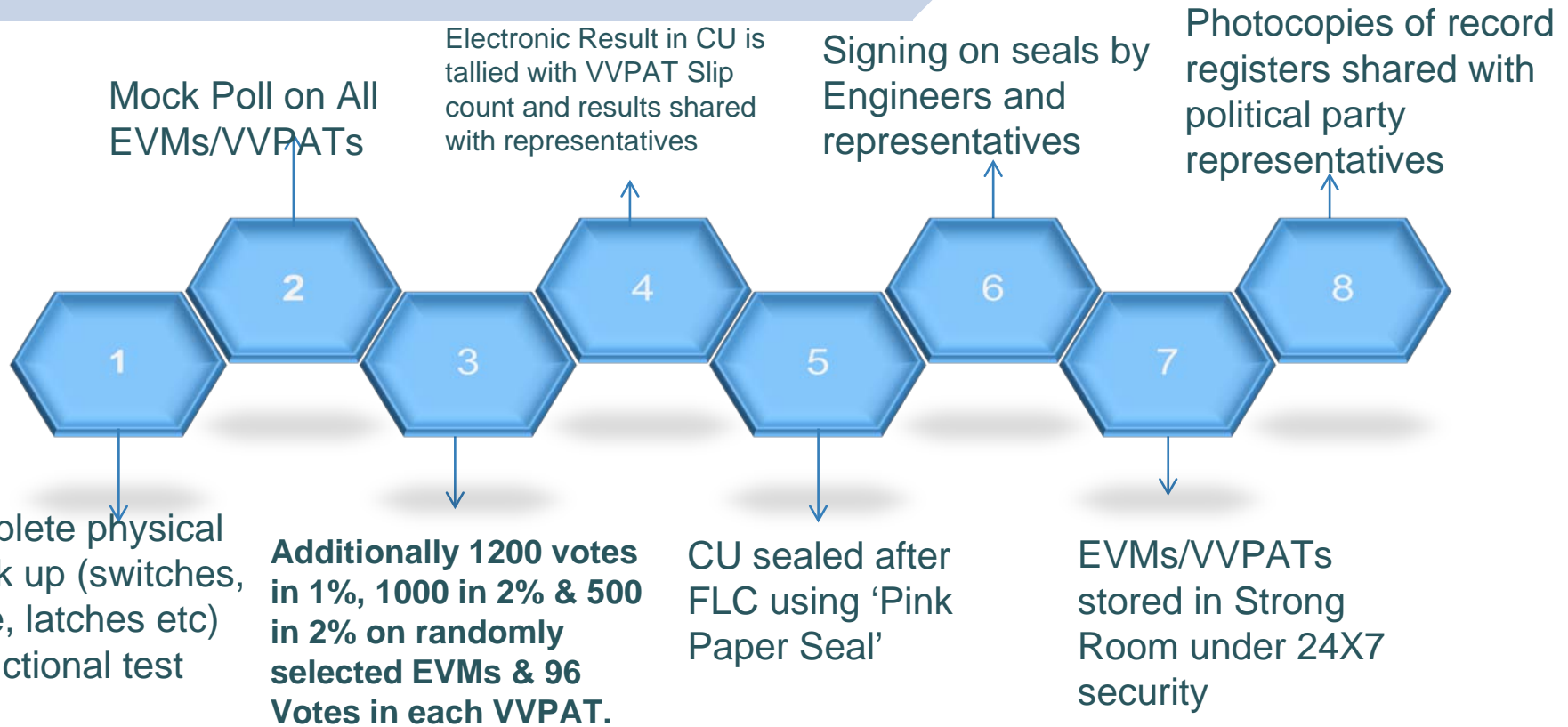


### 3. FIRST LEVEL CHECKING (FLC)

- FLC in the presence of representatives of political parties.
- Fully sanitized hall under videography and full security
- Full functionality and behavioural check is done.
- Defective EVMs are kept aside and not used in election
- Recorded in ETS



# FLC PROCESS



## 4. CANDIDATE SETTING

### The Process

Insert ballot paper in the Ballot Unit & Set Number of Candidates

Seal Ballot Unit

Mock Poll on Every EVM + 1000 vote on 5% EVMs



### Security Measures

- 1 Done **after finalization** of the names of contesting candidates
- 2 **Fully sanitized hall** under videography and full security.
- 3 Done in the **presence of candidates** or their agents.



## 5. RANDOMIZATION



- EVMs are **Randomized twice** using EVM Tracking Software (ETS).
- Only FLC approved EVMs as per ETS get picked up for first randomisation

### 1st Randomization



- Done after FLC
- To allocate EVMs available in district, randomly, to a particular AC.
- In presence of representatives of political parties.
- List of AC-wise Randomized CU/BU and the training EVMs shared with political parties.

### 2<sup>nd</sup> Randomization

## 5. RANDOMIZATION



- EVMs are **Randomized twice** using EVM Tracking Software (ETS).
- Only FLC approved EVMs recorded in ETS get picked up for first randomisation

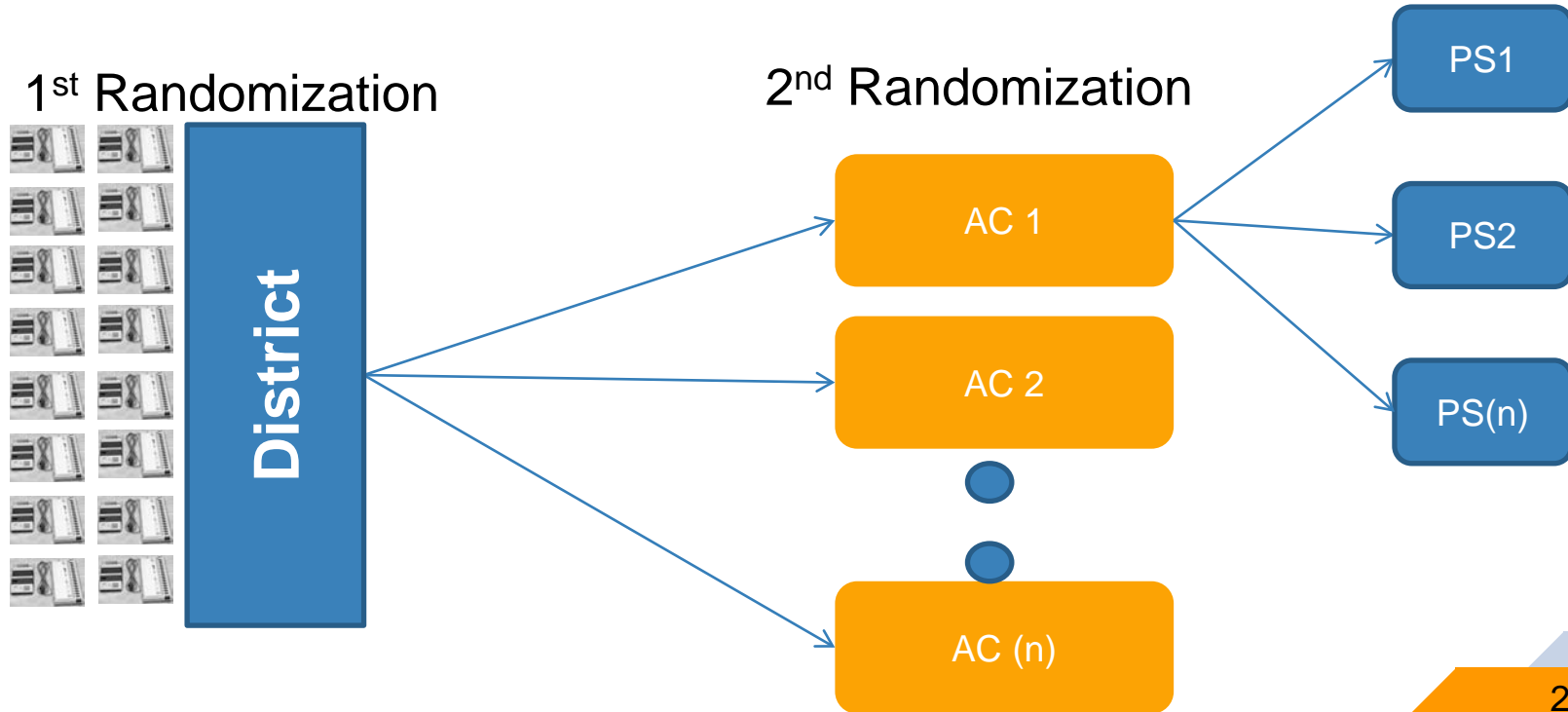
### 1st Randomization

### 2<sup>nd</sup> Randomization



- Done just before 'candidate setting'.
- To allocate EVMs available in an AC to specific polling stations.
- In presence of candidates/election agents and list shared.

# 5. RANDOMIZATION



# RANDOMIZATION- THE FOUNDATION OF EVM SECURITY



- Till first randomization- no one knows which EVM is going to which AC
- Till nomination finalisation- no one knows the sequence of names on the ballot paper
- Hence, till candidate setting no one (not even RO/DEO/CEO/Commission) knows which button on which BU will be assigned to which candidate, making even an attempt to tamper absolutely futile.
- Till 2nd Randomization- no one knows which EVM will go to which PS
- Added to this is the 3 stage Randomization of polling station officials.

## 6. POLL DAY MOCK POLL



- Before start of actual poll, Mock poll with at least 50 votes in the presence of candidates/their agents.
- Mock poll data is erased and shown to the agents.
- The Presiding Officer issues the Mock Poll Certificate with signature of the representatives of candidates.

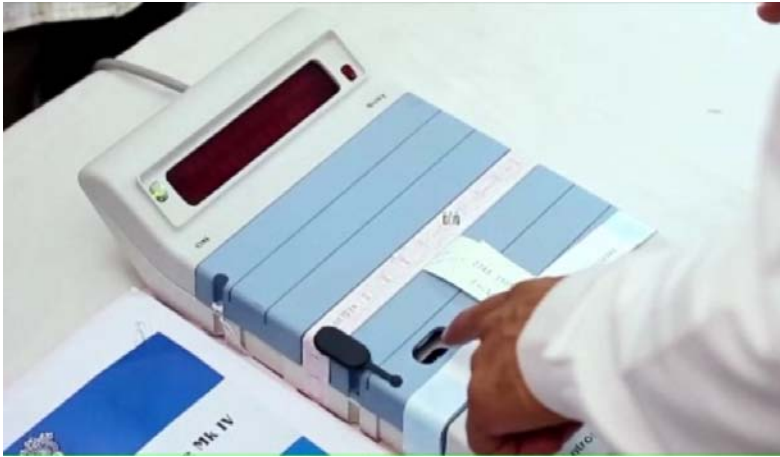
## 7. POLL DAY CHECKS

- Polling Agents
- CAPF, Micro-Observers, Webcasting/CCTV
- Frequent visits by Sector Officers and other senior officers, including Observers
- 2 hourly reporting of votes polled
- Media





## 8. POLL CLOSURE & TRANSPORTATION



Poll Closed on EVM by  
pressing CLOSE button  
on CU



## 8. POLL CLOSURE & TRANSPORTATION



EVMs sealed in carrying cases  
and polling agents sign on them.

## 8. POLL CLOSURE & TRANSPORTATION



The machines are transported back to the reception centres under proper armed escort. Candidates' representatives are allowed to follow them

## 8. POLL CLOSURE & TRANSPORTATION



- EVMs are kept in strong room, sealed in the presence of the Candidates and Observer
- Facilitation for Candidates to watch the Strong Room 24/7
- *Starting from FLC of EVMs to Counting of votes, EVMs are kept in Strong-room with full 24/7 security*



## 9. STORAGE & SECURITY



### Non- Election Period

### Election Period

### Post- Election Period



- EVM storage warehouse with only one entry point.
- Other doors or windows sealed using brick-masonry or concrete.
- Entry secured by a double lock system.
- The keys held jointly by two separate officers, nominated by the DEO.
- 24X7 security arrangement.
- Annual Physical Verification of entire stock by ECI and tracked through ETS

## 9. STORAGE & SECURITY



Non- Election Period

Election Period

Post- Election Period



- EVMs are stored in a strong room in the presence of representatives of Political Parties, under videography.
- Training EVMs are kept in a separate strong room
- After Candidate Setting EVMs are again stored in Strong Room
- EVMs are taken out only on the day of dispersal of polling parties.
- Candidates or their agents and ECI Observers are present through out this process and minutely monitor the same.



## 9. STORAGE & SECURITY



Non- Election Period

Election Period

Post- Election Period



- EVMs are escorted back to the strong room post poll and remains under double lock
- Candidates allowed to put their own locks
- Two cordoned round the clock security arrangements for the strong rooms having polled EVMs
- The CPF secures the innermost perimeter immediately outside the strong room and the State Armed Police secures the outer perimeter.
- 24/7 security arrangement for unused EVMs also.

## 10. COUNTING DAY PROTOCOL

- On the day of counting, strong room opened in the presence of Candidates, RO and Observer under videography.
- Round-wise CUs are brought to the counting tables.
- Unique ID number of the CU & the signed seals are verified and shown to the polling agents.
- EVMs & VVPATs are stored back in Strong Room in the presence of candidates/their representatives till the completion of the Election Petition period.



# ELECTION PETITION PERIOD

REGISTERING COMPLAINT

# ELECTION PETITION PERIOD



Election Petitions can be filed within 45 days of result declaration

EVMs (BU+CU) & VVPATs remain under sealed conditions till EP position is ascertained.

EVMs under EP, along with VVPAT slips, are moved to a separate Strong Room with the approval of the High Court.

All VVPATs & Remaining EVMs not in EP are now free for re-use.

# DEBATE AROUND EVMs-EXPLAINED!

CLARIFICATION OF ALL ISSUES



# DEBATES AROUND EVM

How EVMs are registering votes only for BJP: Kejriwal

Continued from page 1  
Congress and AP staged a protest, demanding that the chief electoral officer (CEO) of Andhra Pradesh (Shakti) be removed. Kejriwal sought report from the chief secretary regarding the officials. The state's chief electoral officer (CEO) of Andhra Pradesh (Shakti) demanded that every single EVM must be checked meticulously. "If some EVMs can be tampered with, many others may also be tampered with. These reports are shocking and raise doubts about the essence of democracy in the country. This means that if the machines are tampered with, no matter who gets the votes, the lotus will bloom in the hands of the BJP," he said. "The essence of democracy is that no cheating takes place. We need to find the fault in EVMs, the software and hardware, and MH-Who is tampering with the software and how is it tampered," he said.

Shocking aspect of the Election Commission's...  
Democracy at Risk!  
Can we trust our machines? Voting...  
GVL Nazamima Rao

**Hacked EVM**  
**Vote Stuffing after Poll Closure**

**Memory Manipulation**  
EVM HACKING  
ELECTION COMMISSION  
BJP  
AAP

**Remotely Altered Control Unit Display**

**Replaced Microcontroller or Memory chips**

**Altered software code**

**International Comparison**



## NO POSSIBILITY OF EVM HACKING

**Hacking'** is unauthorised access to or control over computer network security systems for some illicit purpose

In the case of ECI EVMs, the word '**Hacking**' is **not applicable** for following reasons:

- The EVM is a **stand alone** machine and is not connected to any network through wire or wirelessly
- The SW programme in the OTP Microcontroller can **neither be read nor modified**

# NO POSSIBILITY OF REMOTELY ALTERED CU DISPLAY THROUGH WIRELESS COMMUNICATION

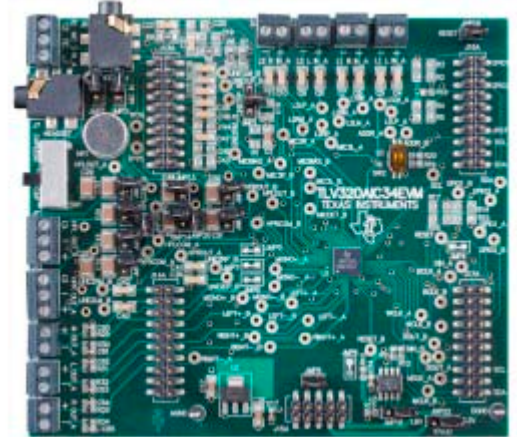
- It is alleged this can be done by either replacing the original display module with another display fitted with a wireless device or inserting an extra circuit board which can communicate with an external unit via a wireless device and tamper the result by controlling the CU display used for declaring the result
- Such a modification would require unfettered access to the EVM after FLC – **Ruled out.**



# MEMORY MANIPULATION RULED OUT



- It is alleged that voting data can be altered by clipping a Memory Manipulator IC to the memory chip where Vote data is stored. This would need,
  - Full and free access to CUs after the Polling is over- **Ruled Out !!**
  - Breaking the seals and locks of the strong room in the presence of two layers of security plus the representatives of the candidates camping near the strong room- **Ruled Out !!**





# REPLACEMENT OF MICROCONTROLLER/MEMORY CHIP or MOTHERBOARD BEFORE POLL/COUNTING IMPOSSIBLE

## Administrative Safeguards

- Chip replacement would require access to EVM Warehouses – **Ruled Out**
- Any chip replacement before FLC will get caught during FLC
- Chip Replacement after FLC would require access to Strong Rooms and breaking of EVM Pink Paper seals– **Ruled Out**

## Technical Security

- BUs and CUs communicate only amongst themselves and go into error mode if connected to any other machine. Thus, **any modified EVM (with microcontroller /memory changed) would not be usable** even if someone is able to hypothetically bypass security arrangements and modify EVM

# TAMPERED SOURCE CODE “TROJAN” RULED OUT

- It is alleged that Trojan can be introduced in following manner
  - by reprogramming the chip, or
  - by the chip manufacturer during fusing of the software.
- Re-programming **Ruled Out** as these are OTP chips.
- Code tampering by the chip manufacturer **Ruled Out** as it will get caught during the code integrity check.



# NO POSSIBILITY OF VOTE STUFFING AFTER POLL CLOSURE



## **Administrative safeguards**

- Poll closed by pressing the “CLOSE” button on the CU after last vote, Representatives of candidates who are present signs on the seals
- EVM seals checked on counting day

## **What if seals broken and votes stuffed while transporting?**

- EVM does not accept any votes after CLOSE button pressed in CU

## **What if CLOSE button not properly pressed and Votes Stuffed while transporting?**

- Poll Closure time recorded in the PO's diary and any votes polled in the EVM after this time can be identified due to time stamping of key presses

# ILL INFORMED DEBATE CONFUSING VVPAT FAILURE WITH EVM DEFECT



- VVPAT defects in field wrongly dubbed as 'EVM failure'
- EVMs in use for last 2 decades: Usage stabilized, Personnel trained, familiarized and comfortable, failure rate stabilized around 1-2%
- VVPAT is a new machine: essentially a mechanical printer with lots of sensors
- Production and field usage still being stabilized.
- Field machinery coming to grips with the new machine: capacity building a work in progress: many failures due to improper handling.
- During polls: If VVPAT is defective, only VVPAT is changed, NOT an EVM problem per se.
- VVPAT failure rate around 5-6%
- Need effective awareness and IEC programmes for educating the media and Public.

# Why Other Countries Discontinued EVMs



ECI EVM	Foreign EVM
Standalone	Mostly networked
Manufactured in Premium PSUs	Manufactured entirely by private entities
Verified and certified by an independent Technical Experts Committee	No such robust and independent certification/ checks
Data is stored internally and not transferrable by any device	Voting data recorded in the DRM is transferred by means of CD, etc
Full end to end security protocol and administrative safeguards for the use, storage, transportation and tracking	No such protocols, e.g. in Ireland
Administrative and physical security as per legal framework across the country.	No such legal framework, e.g. in Netherlands
Voter verifiability and auditability of every vote cast	Lack of such facility in the NEDAP machines- un-Constitutional by German Supreme Court as lacked public examinability

# Country Specific Details (as per Status Paper)



## Germany:

In Germany, the e-voting machines manufactured by NEDAP were used in between 2005 – 2009 before it came under criticism and finally discontinued. The Federal Constitutional Court of Germany ordered the discontinuation of the use of NEDAP machines in 2009 because of the below-mentioned reasons:

- ⌚ The use of NEDAP electronic voting machines violated the principle of the public nature of elections (Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law) that requires that all essential steps in the elections are subject to public examinability unless other constitutional interests justify an exception.
- ⌚ It also observed that “it must be possible for the citizen to check the essential steps in the election act and in the ascertainment of the results reliably and without special expert knowledge”.

# Country Specific Details (as per Status Paper)



## The Netherlands

Electronic Voting was used in The Netherlands in between 1990-2007. The voting machines were manufactured by a private Dutch-company called NEDAP (*Nederlandse Apparaten Fabriek NV*). In 2006, the government ordered an independent testing of the voting machines. Two independent commissions, The Voting Machines Decision-making Commission and the Election Process Advisory Commission (EPAC) were also established on December 19, 2006 and January 18, 2007, respectively, to review the security and reliability features of NEDAP machines.

Following the observations of the two Commissions, the use of NEDAP machines and electronic voting was discontinued in 2007 on the following grounds:

- The Ministry of Interior and Kingdom Relations (MOIKR) of The Netherlands lacked adequate technical knowledge vis-à-vis the NEDAP machines, leading officials to depend on external actors for the conduct of elections.

# Country Specific Details (as per Status Paper)



## The Netherlands

- Technology vendors became part of the decision making process and the ministry was not in a position to exercise effective oversight.
- The Dutch Organization for Applied Scientific Research (*Toegepast Natuurwetenschappelijk Onderzoek*, TNO) certified and tested these machines following “outdated standards” which were not immune to modern IT and security threats.
- Moreover, the certification and testing reports were not made public depriving independent experts to verify the analysis.
- The legal framework, particularly the necessary security requirements, was inadequate to deal with the specificities of the electronic voting process.

# Country Specific Details (as per Status Paper)



## Ireland:

NEDAP machines were used in Ireland in between 2002 – 2004. The use of these machines was questioned following which two independent commissions were set up. The two Commissions on the *Secrecy, Accuracy and Testing of the Chosen Electronic Voting System*, concluded the NEDAP machines could not be used in elections in Ireland on the following grounds:

- Inadequate technological safeguards
- Insecure transfer of data by the use of CDs
- Absence of a comprehensive independent end-to-end testing, verification and certification by a single accredited body
- Inconsistencies in physical security of machines across constituencies
- Absence of a clear policy guideline via-a-vis storage, transport, set-up, use and disposal of voting equipment; and
- Absence of comprehensive electronic register to record the identity, location and movement of the electronic voting devices.

# Country Specific Details (as per Status Paper)



## **United States of America:**

In 2000, after the dispute on the voting method in the USA presidential elections, the voting method was reviewed (Esteve, Goldsmith, & Turner, 2012: 185). Accordingly, Direct Recording Electronic (DRE) Systems (like the widely used AccuVote TS developed by Premier Election Solutions, commonly called Diebold) were introduced. DRE Systems uses “one of three basic interfaces (pushbutton, touchscreen or dial)” through which “voters record their votes directly into computer memory. The voter’s choices are stored in DREs via a memory cartridge, diskette or smart card...Some DREs can be equipped with Voter Verified Paper Audit Trail (VVPAT) printers...” Currently, in the USA, the Direct Recording Machines are used in 27 states, among which paper audit trails are used in 15 states. The other voting methods include: Optical Scan Paper Ballot Systems, Ballot Marking Devices, and the Punch Card Ballot.

# Country Specific Details (as per Status Paper)



## Other countries:

In Brazil, the machines used in elections are called 'electronic ballot boxes' which are stand-alone direct electronic recording systems. In Venezuela, SATIS (Smartmatic Auditable Election Systems) voting machines are used which were fully implemented across the nation in 2004. (Esteve, Goldsmith, & Turner, 2012: 185)

# ASPERSIONS VS CONFIDENCE

Between MAR-DEC 2017

## BHIND FINDINGS



Commission's enquiry found 4 buttons of BU pressed in the following order and VVPAT printed corresponding slips

Button no	Symbol	Name of Candidate
03	Handpump	Raju Pal
04	Lotus	SatyaDev Oanchori
03	Handpump	Raju Pal
01	Hand	Ambuj Shukla

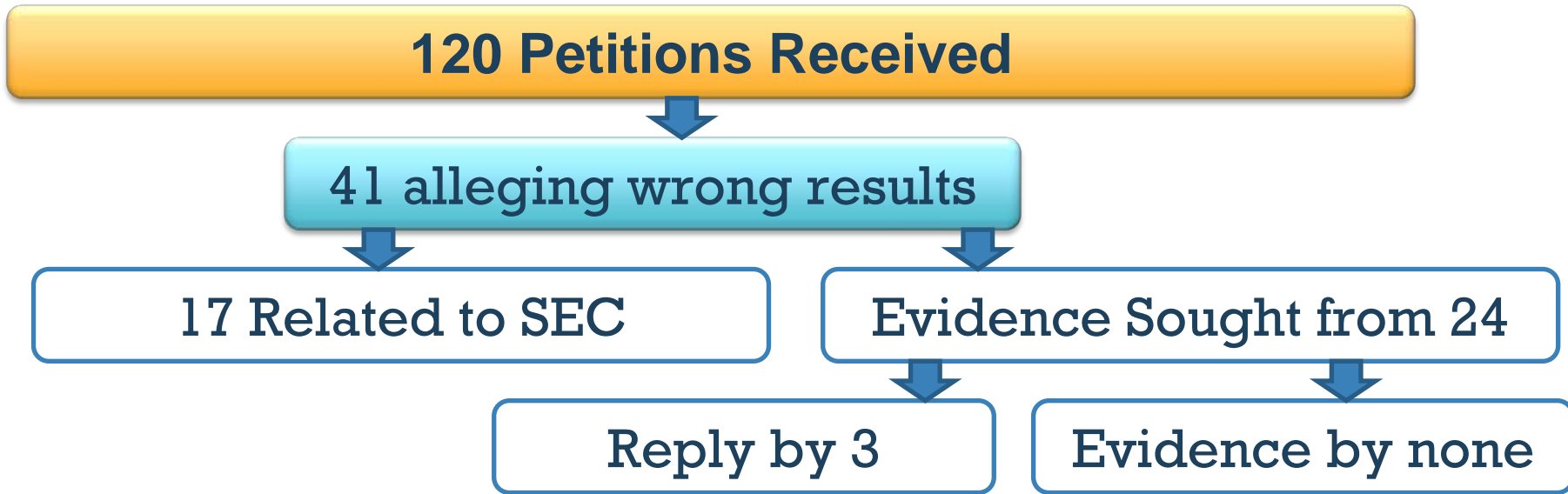
**It is pertinent to mention here that is it completely false to say that the multiple times slips of lotus were printed during the demo on 31<sup>st</sup> March as alleged**

## DHOLPUR FINDINGS



**It was alleged that in 18 EVMs votes went to only one Party irrespective of the buttons pressed. However no specific complaint received till date by the Commission. 10 BUs and 10 CUs found defective and replaced.**

Between March-May 2017



# PROTOCOL FOLLOWED ON DEFECTIVE EVMs



# DEFECTIVE EVM PROTOCOL



## Defective EVMs

Includes EVMs that fail to function due to any mechanical, structural or physical defect like faulty switches, broken button, faulty connections etc. However, these NEVER give Wrong Result.

- EVMs are checked for defects during FLC, candidate setting, before start of poll and during poll.
- Serial Numbers and defects of these EVMs are noted and EVMs are sent to the manufacturers for analysis and repair.
- Manufacturers follow same security protocols during repair as they do for manufacturing new EVMs.

# PAST JUDGEMENTS

INDIAN Vs Foreign EVMs



## JUDICIAL SCRUTINY

<b>Total No. of Court Cases on EVMs:</b>	<b>37</b>
<b>Judgments given:</b>	<b>30</b>
<b>Judgments awaited:</b>	<b>07</b>

# JUDGEMENTS SUMMARY



## **Madras High Court 2001**

*“There is also no question of introducing any virus or bugs for the reason that the EVMs cannot be compared to personal computers.”*

## **Karnataka High Court 1999**

*‘This invention is undoubtedly a great achievement in the electronic and computer technology and a national pride’.*

# JUDGEMENT SUMMARY



## **Kerala High Court 2002**

In one EP the High Court recorded its appreciation on the efficiency of the mechanism of detecting votes cast by impersonators. Upheld by the Hon'ble Supreme Court in 2003.

# Forensic Checking



## **Bombay High Court: Order dated 23.02.2018:**

In EP No. 15 of 2014, the Bombay High Court ordered a detailed forensic examination of the EVMs from CFSL, Hyderabad for checking any manipulation etc. The CFSL report clearly ruled out any tampering, alteration or manipulation in the EVMs, the report accepted by Hon'ble High Court and petition dismissed.

# VOTER VERIFIABLE PAPER AUDIT TRAIL (VVPAT)

# VVPAT



**VVPAT- allows the voters to verify that their votes are cast as intended.**



# VVPAT



- Voter Verifiable Paper Audit Trail is an independent system, attached with the Electronic Voting Machines, that allows the voters to verify that their votes are cast as intended.
- When a vote is cast, the elector shall be able to view through the transparent window of the VVPAT, the printed paper slip showing the **serial no**, **name** and the **symbol** of the candidate of his choice.
- The slip remains exposed through the window for 7 seconds, after which it automatically gets cut and falls in the sealed drop box of the VVPAT.
- Since June 2017, VVPATs are being used in all Elections.

## VVPAT Complaint – Rule 49MA



In case a voter complains of wrong printing by VVPAT:

- He will report to Presiding Officer
- Presiding Officer will take a declaration explaining that if found false he can be penalized.
- PO will then record in 17A and permit him to cast a 'test vote' in presence of PO and Polling Agents
- If found false PO will record in 17A and 17C so that the test vote is not counted
- If found true then PO will stop poll and report to RO

## VVPAT RECOUNTING PROCESS

- Counting of votes according to Rule 56C of Conduct of Election Rules, 1961
- After announcement of result any candidate/ his agent may apply in writing to the RO for counting of paper slips of VVPAT under **Rule 56D**.
- The RO shall pass a speaking order on whether the slip counting to be allowed.
- **7** instances RO has allowed slip counting since 2017.

## VVPAT RECOUNTING PROCESS

- VVPATS were used in all 5 states in early 2017 but in Goa alone, recount requested under 56D and permitted by RO in 4 Polling Stations.
- Count exactly matched in all the 4 recounts done
- 100% VVPAT coverage done in Gujarat and HP in Oct-Nov 2017. Only 1 request under 49MA, verified as per law, found incorrect. FIR lodged against the complainant.
- 100 % VVPAT coverage also done in Nagaland, Meghalaya, Tripura and Karnataka.
- Pilot verification of VVPAT slips of 1 (ONE) randomly selected PS per AC done in all States- 100% match, as expected, was found. So far, VVPAT slip count done in 839 randomly selected PS.



## PRESENT STATUS

- In the light of technical security features and administrative safeguards, Commission has full confidence on its EVM system
- Commission committed to deploy VVPATs in all elections as per commitment given to Hon'ble Supreme Court
- 40 lakh units (BU, CU, VVPAT) under production at a cost of Rs. 5626 cr.

## Why Going Back to Ballot not a Solution

1. Retrograde step in the era of Technology when all transactions are done with technology
2. Average around 2000 invalid votes in each Constituency when ballots used
3. Vote stuffy was very easy with Ballot papers, muscle power used to rule
4. Counting of Ballot Papers was always prone to errors



**THANK YOU**