
# REPORT ON I-VOTING PILOT TEST IN 35 CONSTITUENCIES HELD ON 14TH OCTOBER, 2018

**ELECTION COMMISSION OF PAKISTAN**

# TABLE OF CONTENTS

## BACKGROUND

The subject of grant of right of vote to Overseas Pakistanis remained under consideration in the Election Commission of Pakistan (ECP) since long. ECP had established a Directorate for Overseas Voting in its Secretariat at Islamabad. It is constantly involved in consultation and research on the subject. The consultative process was not only confined to the local stakeholders i.e. Political Parties, Civil Society Organizations and Media, but is also extended to the associations of Overseas Pakistanis.

ECP has been working to devise the mechanism for granting the voting rights to the Overseas Pakistanis since 2015. In order to develop a workable, effective and transparent mode of voting for Overseas Pakistanis, the Honourable Election Commission had constituted a Special Committee on Overseas Voting to conduct the Feasibility Study of Overseas Voting, In addition to this the 'Sub-Committee of Parliament on Electoral Reforms' headed by Dr. Arif Alvi, Ex-MNA also desired that ECP may conduct Mock exercises for Overseas Voting by using the following two modes, Postal Ballot (Online Re-registration, Voting through Postal Ballots), IVR Tele Voting, Voting through Telephone (Interactive Voice Response). However the life cycle of Mock Poll using Postal Ballot and IVR was not successful and the reports were also shared with the Parliamentary Committee on Electoral Reforms.

## INTERNET VOTING TASK FORCE (IVTF)

The Honorable Supreme Court of Pakistan convened a session on 12th April, 2018 (Reference Constitution Petition No.2/2018-SCJ) pertaining to the voting rights of Overseas Pakistanis. This session was presided over by the Honourable Chief Justice of Pakistan, Justice Saqib Nisar, and included members of various political parties, IT experts from Pakistani universities, concerned citizens, and members of the media. The purpose of the session was to discuss the I-Voting platform developed by NADRA that would allow overseas Pakistanis to cast their votes. As a result, on directions of the Honourable Supreme Court of Pakistan, the Election Commission of Pakistan constituted a Task Force on 19th April, 2018 to undertake a technical audit of the iVOTE platform. Following were the recommendations of the Internet Voting Task Force:-

> "Internet voting, if needed, be deployed in a piecemeal organic manner starting with multiple small non-political elections (e.g. trade organization, bar councils,

engineering bodies, etc.), followed by small-scale political elections (intra-party elections, local government polls, bye-elections), and slowly expand in scope.

This strategy allows for review and further improvement at every stage in terms of usability and security. The electorate also gets a chance to adjust to this new system and provide valuable feedback. Verifiability measures could be incorporated piecemeal at different stages of the election process. The technical challenges and threat model for deploying such a system also become clear and system administrators develop valuable experience in the process.

Additionally, in the event of technical glitches, hacks, or system failure, the political risk is proportionately restricted. Furthermore, if there are legal challenges to this system (as have been observed in several countries including Germany, India, and Poland), then they can be addressed in a timely manner without wasting resources on a very large deployment.

It was also recommended that periodic security audits of Internet voting system as well as regular sponsored hackathons and bug bounties (similar to those conducted in India and at DEFCON) where hackers are invited to attack the system for monetary reward."

The detailed report of Internet Voting Task Force is attached at **"Annexure-A"**.

**THE JUDGEMENT OF HONOURBLE SUPREME COURT OF PAKISTAN FOR CONDUCT OF PILOT PROJECT PASSED ON 17th AUGUST, 2018**

In the **Constitution Petitions No. 74 to 79 Of 2015, 49 to 56 of 2016 and 2 of 2018 and Civil Misc. Applications No. 4292 of 2017 and 162 of 2018 (Under Article 184 of the Constitution),** the Honourable Supreme Court of Pakistan has directed ECP to conduct pilot project on Internet Voting (I-Voting) on 14th October, 2018 Bye-Elections of 37 constituencies. The detailed Judgment is attached at **"Annexure-B"**. The operative part of the Judgment is reproduced hereunder:-

*"The ECP and NADRA has given presentations to this Court in the foregoing regard and about third party validation that has also been received from independent experts, regarding the safety, integrity, and workability of the system. Based on these representations we prima facie find the mechanism of I-Voting to be safe, reliable and effective for being utilized in a pilot project. We are sanguine that the aforesaid proposed rules shall be incorporated in the Election Rules, 2017 to enable overseas Pakistanis to exercise their right of vote in the forthcoming bye-elections. However, we direct the results of the bye-elections and the vote count of the votes cast by the overseas Pakistanis through the I-Voting mechanism shall be kept separately and also secret till the time that ECP satisfied about the technical efficacy, secrecy and security of the votes cast by overseas Pakistanis through the I-Voting System. In case such determination, made on the basis of*

*reasons, is in the negative and the ECP is not satisfied about the integrity, safety and reliability of the systems and votes cast through the same; ECP shall exclude the segregated votes cast by the overseas Pakistanis from the official result of the bye-elections in accordance with the proviso to Rule-84-C(2) supra. This safety feature shall ensure that elections are founded upon verified and authenticated votes only."*

## PROGRESS MADE BY ECP ON OVERSEAS VOTING

With regard to grant of right of vote to Overseas Pakistanis, the following tasks were accomplished by ECP in the manner as follows:-

| S # | Activity Details | Date |
|---|---|---|
| 1. | Letter sent to the UNDP for the preparation of comprehensive Feasibility Report on Overseas Voting for Pakistan | 16-11-2015 |
| 2. | Terms of Reference (TOR) was communicated to UNDP for hiring International Consultants(s) specialized on Overseas Voting | 16-11-2015 |
| 3. | Notification of Special Committee on Overseas Voting | 20-11-2016 |
| 4. | Letters were sent to following Ministries for the nomination for their Focal Persons:-<br>i. Ministry of Finance<br>ii. Ministry of Foreign Affairs<br>iii. Ministry of Interior<br>iv. Ministry of Overseas Pakistanis & HRD<br>v. National Database & Registration Authority (NADRA)<br>vi. Ministry of Information Technology & Telecom<br>vii. Ministry of Law & Justice | 20-11-2015<br><br>11-12-2015 |
| 5. | The "Report on Overseas Voting (Mock Poll)" conducted by Election Commission of Pakistan and the Ministry of Foreign Affairs on the directions of the Sub Committee on Electoral Reforms by following two different methodologies/modes of voting i) Postal Ballot using email ii) Tele Voting (Interactive Voice Response) during the period of Oct-Nov 2015 | 23-11-2015 |
| 6. | Presentation on outcome of the Overseas Voting (Mock Poll) | 24-11-2015 |
| 7. | The ECP designated Director (Research & Overseas Voting) along with his dedicated team to work on "Overseas Voting" | 04-12-2015 |
| 8. | Engaging a Consultant for the propos by UNDP process of hiring complete | January, 2016 |
| 9. | Michael burke UNDP's Consultant completed writing Feasibility Report on Overseas Voting for Pakistan | March, 2016 |
| 10. | Feasibility Report on Overseas voting for Pakistan shared with Parliamentary Committee on Electoral Reforms | March, 2016 |

| | | |
|---|---|---|
| 11. | Meeting of ECP's Committee held to discuss possibility of Pilot Project through phone system and Discussion with Sub-Committee regarding proposed pilot project using internet voting system on 13-04-2016 | April, 2016 |
| 12. | The "brief report on Mock Exercise held National Assembly Secretariat using internet Voting System on 21st & 22nd April, 2016 | April, 2016 |
| 13. | Response to Special Report of the Senate Standing Committee on Overseas Pakistanis and human recourse Development on the problem being faced by Overseas Pakistanis | 11-07-2016 |
| 14. | NADRA Briefing to Election Commission on I-Voting System for Overseas Pakistanis as desired by Sub-Committee of Parliamentary Committee on Electoral Reforms | 20-04-2017 |
| 15. | Meeting held with NADRA for provision of PS-114 NICOP card holder data alongwith demo of I-Voting software for Overseas | 24-05-2017 |
| 16. | Letter sent to NADRA for obtaining data and software of i-Voting system for Overseas as a Pilot Project | 05-06-2017 |
| 17. | NADRA's reply to ECP letter about regret of not having any I-Voting solution | 09-06-2017 |
| 18. | Enactment of the Election Act, 2017 (Section-94) by Parliament | 02-10-2017 |
| 19. | Letter sent to NADRA to conduct Pilot testing of Overseas Voting under Section-94 of Election Act-2017 and share Draft Contract | 21-11-2017 |
| 20. | NADRA’s draft Contract received for Pilot Testing to ECP | 07-12-2017 |
| 21. | Overseas Voting Committee re-constituted | 05-01-2018 |
| 22. | On the directions of the Supreme Court of Pakistan, the ECP constituted a Task Force to undertake a technical audit of the I-VOTE platform | 19-04-2018 |
| 23. | Submission of Report by the Internet Voting Task Force to the Honourable Supreme Court of Pakistan and ECP | 31-05-2018 |
| 24. | Supreme Court order Issued to Conduct Pilot Project on 14th October 2018 in Bye-Elections of 35 constituencies | 17-08-2018 |
| 25. | Framing of Rules with reference to I-Voting | 08-10-2018 |
| 26. | Pilot Testing of I-Voting System developed by NADRA in 35 Constituencies | 14-10-2018 |

# Timeline of Key Developments and ECP Progress on Overseas Voting

**Nov 2015**

UNDP engaged to prepare comprehensive Feasibility Report on Overseas Voting for Pakistan in response to calls for an objective, third party analysis of the issue

**Nov-Dec 2015**

ECP-led Special Committee on Overseas Voting is established; focal persons from various government ministries nominated

**Nov 2015**

Feasibility Report on Overseas Voting developed by UNDP's Michael Burke shared with Parliamentary Committee on Electoral Reforms. Report examines mechanisms in other countries and recommends that ECP should proceed with caution and test different options. Report also concludes that any mechanisms should be tested through embassies in a controlled environment rather than the entire diaspora.

**Mar 2016**

ECP and Ministry of Foreign Affairs submit report on directions of the Parliamentary Sub Committee on Electoral Reforms examining two overseas voting options:
i) Postal Ballot via email and
ii) Tele Voting (Interactive Voice Response).
Report concludes these mechanisms are not foolproof or practicable and recommend that committee explore alternatives, study practices in other countries.

**Apr 2016**

PCER member Arif Alvi writes to Zahid Hamid recommending that internet voting should be rolled out for overseas Pakistanis

**Apr 2016**

ECP Committee explores pilot project options, tests internet voting system in National Assembly Secretariat and prepares a report

**Jul 2016**

ECP responds to Special Report of the Senate Standing Committee on Overseas Pakistanis and Human Recourse Development on the problem being faced by Overseas Pakistanis, highlights findings of Postal ballot and IVR pilots plus UNDP report. Discussion then shifted to PCER to consolidate overlapping efforts.

**Apr 2017**

NADRA Briefs Election Commission on I-Voting System on direction of the Sub-Committee of PCER. Technical and academic experts are invited to briefing, chaired by Chief Election Commissioner. There is unanimous recommendation from these stakeholders against implementation.

**May-June 2017**

ECP reaches out to NADRA to obtain data and software to pilot I-Voting in PS-114 by-election scheduled for July. Pilot ultimately not undertaken as NADRA cites lack of preparation and time.

**Jan 2018**

ECP Overseas Voting Committee re-constituted in response to numerous petitions to Supreme Court calling for overseas voting facility to be provided to all eligible voters in General Elections 2018

**Oct 2017**

The Elections Act, 2017 passed by Parliament, includes requirement for ECP to test overseas voting through pilots and share assessments/findings with the government (Section 94)

**Nov-Dec 2017**

ECP works with NADRA to finalize terms of engagement for pilot testing in compliance with new law

**Oct 2018**

Pilot Testing of I-Voting System in 35 Constituencies

**Oct 2018**

ECP determines no major technical issues in pilot and counts all votes in final results

**Mar 2018**

Contract signed with NADRA for pilot testing

**Apr 2018**

On the directions of the Supreme Court of Pakistan, ECP constitutes a Task Force to undertake a technical audit of the IVOTE platform

**May 2018**

Internet Voting Task Force submits report to Supreme Court of Pakistan and ECP highlighting significant risks and weaknesses of IVOTE, calls for gradual testing of other options such as end-to-end (E2E) verifiable voting

**Aug 2018**

Supreme Court orders the pilot of IVOTE in 14th October 2018 Bye-Elections, with votes to be counted in results unless there are valid controversies. ECP files Civil Miscellaneous Application objecting to the order.

**Aug-Sep 2018**

ECP rapidly mobilizes to register eligible overseas voters in 35 constituencies, conducts outreach to increase awareness

## IMPLEMENTATION OF I-VOTING PILOT TEST IN BYE-ELECTIONS IN 35 CONSTITUENCIES HELD ON 14th OCTOBER, 2018

With reference to pilot testing of Overseas Pakistanis Voting in Bye-Elections of 35 constituencies held on 14th October 2018 as per Section 94 of Election Act, 2017 by using Internet Voting System, the following different procedure/activities were performed during the Pilot Project. Hon'ble Election Commission had approved the timeline and had directed NADRA to perform the pilot test:-

Timelines for I-Voting Pilot (Bye-Elections 14 Oct 2018)

| S # | Activities | Timelines | Responsibility | Compliance by NADRA |
|---|---|---|---|---|
| 1. | Re-Constitution of Overseas Voting Committee | By 20th August, 2018 | ECP | N.A. |
| 2. | Election Schedule / Identification of Constituencies for I-Voting | | ECP | N.A. |
| 3. | Business Requirement Document (BRD) as per Electoral Reforms Committee | | ECP & NADRA | Approval provided by ECP for implementation by NADRA on 29th August 2018. |
| 4. | Implementation of recommendations by Task Force (Technical) | By 1st to 15th September, 2018 | NADRA & ECP | Technical Recommendations as practically possible and applicable were implemented by NADRA as per BRD approval of ECP. |
| 5. | User Acceptance Test of I-Voting | | ECP | Approval provided by ECP on 29 August 2018. |
| 6. | Media Campaign for voters awareness | | ECP | N.A |
| 7. | Provision of Form-33 List of Contesting Candidates to NADRA | | ECP | N.A |
| 8. | Provision of Electoral Rolls Data | | ECP | N.A |
| 9. | Integration of Electoral Rolls Data | | NADRA | With per approval of ECP, Electoral Rolls data was integrated by NADRA |
| 10. | Letters to Ministry of Foreign Affairs and NADRA for further dissemination message about I-Voting pilot testing and voter's awareness campaign | | ECP, M/o Foreign Affairs & NADRA | NADRA updated messages/banners on NADRA official website, PakID website, displayed A4 size banners, 6x4Panaflex Banners, Standees at NADRA |

| | | | | |
|---|---|---|---|---|
| | | | | counters/centers abroad operative at Pakistan Foreign Missions. |
| 11. | Demonstration of I-Voting to Hon'ble Election Commission before implementation | 30th September, 2018 | NADRA & ECP | Demonstration to Hon'ble Election Commission of Pakistan was provided on 30th August 2018 before Implementation. |
| 12. | Quality Assurance and Stress Testing of Application | 1st September, 2018 | NADRA & ECP | Quality Assurance and Stress Testing of I-Voting System was conducted before Implementation. Reports were submitted to ECP on 3rd September 2018. |
| 13. | Voter secrecy and result encryption/Decryption of data | | NADRA & ECP | Full Admin Control/Users were provided to ECP by NADRA on 31st August 2018. Key generation, Election Opening (Encryption) was done by ECP on 12th October 2018. Election Closure (Decryption) was done by ECP on 14th October 2018. NADRA provided technical assistance/ guidance only during these events, on request of ECP. |
| 14. | Hosting deployment and maintenance of Application | | NADRA & ECP | NADRA deployed, hosted and maintained the Application as agreed with ECP. |
| 15. | Training session of ECP Officers for running I-Voting | | NADRA & ECP | Training provided by NADRA on 31st August 2018. |
| 16. | Voter's Re-registration | 1st to 15th September, 2018 | ECP & NADRA | Registration for I-Voting initiated on 1st September 2018. As per ECP directives received on 14th September 2018, Registration process was concluded on 17th September 2018 at 0900hrs. |
| 17. | Call Center Support | 1st September, 2018 upto after Poll Day) | NADRA | As per approved BRD, Contact Center (email based support) was operational throughout the duration of Registration Phase till Election Day to support all complaints of eligible voters. Additionally, |

| | | | | |
|---|---|---|---|---|
| | | | | Call Center Helpline was also established between 10-14 October, 2018. |
| 18. | I-Voting Pilot testing report of bye-elections | Within 10 days of poll. | NADRA | Initial Presentation/ briefing to Hon'ble Election Commission by NADRA on 15th October 2018. This report is being submitted in compliance to this action Item of NADRA. |
| 19. | Future recommendations | Within 10 days of the pilot testing report. | ECP | N.A. |

## COMPOSITION OF I-VOTING SYSTEM

I-Voting system comprises of two main components i.e:-

- Voter Verification and Registration
- Voters Passcode and Vote Casting

## VOTER REGISTRATION AND VERIFICATION

For Registration phase, the I-Voting comprises of two main components i.e**.** Voter Verification and Registration System. These components facilitated the approved process that involved email validity check for Account Creation and Voter Eligibility & Verification before completion of Registration.

The system was deployed in Production and made available over the internet for Registration of I-Voting on 1st September 2018. The Registration Phase was due to end on 15th September 2018 (12:00am mid-night), however as per ECP directives, the Registration phase was extended for 33 hours by ECP. A total of 7,419 voters from 35 constituencies were registered with I-Voting till closure of Registration phase.

In order to facilitate the potential voters in the registration phase of I-Voting there were detailed guides and video tutorials available on the I-Voting website. Also, there was an option to contact support team via email through the I-Voting Website.

## VOTER PASS CODE AND VOTE CASTING

This section pertains to issuance of Voter Pass activity (10th – 14th October, 2018) and Vote Casting through I-Voting on Election Day i.e. 14th October, 2018 (8am-5pm Pakistan Standard Time).

The Voter Pass issuance process involved sending system generated Voter Passes through emails to registered voters of I-Voting. As per approved procedure for Vote Casting through I-Voting, the registered voters were required to enter a valid voter pass (for authentication of voter) before they can securely cast their votes through I-Voting. In case the Voter did not receive their Voter Pass, Contact Center and Call Center were operational to resend latest/valid voter pass to registered email address of the voters. Additionally, if Voters felt that their Voter Pass was compromised/stolen, the registered voters were provided with an option to Re-generate a new Voter Pass through system after logging in to their I-Voting account. If a voter regenerated a voter pass, the previously issued Voter Pass was invalidated automatically by the system.

As per the notification of ECP, the By-Elections, 2018 was scheduled on 14th October, 2018. The election time for I-Voting was from 8:00 AM to 5:00 PM Pakistan Standard Time (PST).

In order to ensure the secrecy of vote, the whole process of I-Voting was secured through encryption and decryption of election event. This required ECP to generate the Encryption / Decryption Keys. The encryption key was required to be entered for opening the election event whereas the decryption key was required to close the election event. After decryption and closure of election event, all reports including Form-45 were made available by the system to ECP.

I-Voting website remained available throughout the duration of election time. As per the approved procedure for Vote Casting through I-Voting, all registered voters were required to login to their accounts, provide their Voter Pass and NICOP number (for authentication purpose) and cast their vote on an Electronic Ballot Paper accordingly. The voter was prompted through a message for confirmation before final vote was recorded. This feature was provided to rule out any mistakes done by voter during vote casting. In order to ensure that Voting is kept secret, all data was encrypted and no audit trail of voting was kept by the system.

ECP through Admin Panel of I-Voting, Generated the Keys and opened the Election event on 12 October 2018 for 14th October 2018 By-Election, by entering the Encryption Key. The Election event was closed by ECP on 14th October 2018 (after 5:00 PM) by entering the Decryption Key. All reports including Form-45 were available within 20 minutes, immediately on conclusion of decryption of data process.

A total of 7,364 Voter Passes were issued to all registered voters of 35 Constituencies (of National and Provincial Assembly seats), in which voting through I-Voting was done for Bye-Elections held on 14th October, 2018. These 7,364 voters could cast a total of 7,461 votes. On Election Day, a total of 6,146 Voters casted a total of 6,233 votes for 34 constituencies. There were 87 voters, who casted votes for both National Assembly Seats and Provincial Assembly Seats i.e. NA-103/PP-103 and NA-56/PP-3.

No Voting through I-Voting was done for three Constituencies because:-

- PP-296 Rajanpur-IV and PP-87 Mianwali-III were declared unopposed by ECP;
- No Voter registered with I-Voting for PB-40 Khuzdar-III.

In order to facilitate the Registered I-Voters, detailed guides and video tutorial on "How to Cast Vote" were made available at the I-Voting website www.overseasvoting.gov.pk. Moreover, in addition to the E-mail based support (functioning from 1st September, 2018) through a dedicated Contact Centre, a Help Line was also set up from 10th October, 2018 which remained operational till 14th October, 2018 (The Polling Day) at the given number 0092-51-2778899.

## STATISTICS OF I-VOTING

This section pertains to statistics of I-Voting during the Registration Phase, Voter Passes Issuance and Voting on Election Day. The statistics provided in this section cover the series of events from 1st September, 2018 till 14th October, 2018.

## REGISTERED VOTERS AND VOTES

The set eligibility criteria for I-Voting in the Business Required Document (BRD) was met by 631,909 Overseas Pakistanis for 35 Constituencies in which the Bye-Elections were to be held (11 National Assembly & 26 Provincial Assemblies Seats). A total of 7,419 Voters (From 35 Constituencies) registered themselves for I-Voting to cast their

Vote through Online Voting System. There were no voters registered from PB-40 Khuzdar-III.

These registered I-Voters were scored out from the manual voter lists, which was prepared for Bye-Elections, 2018.

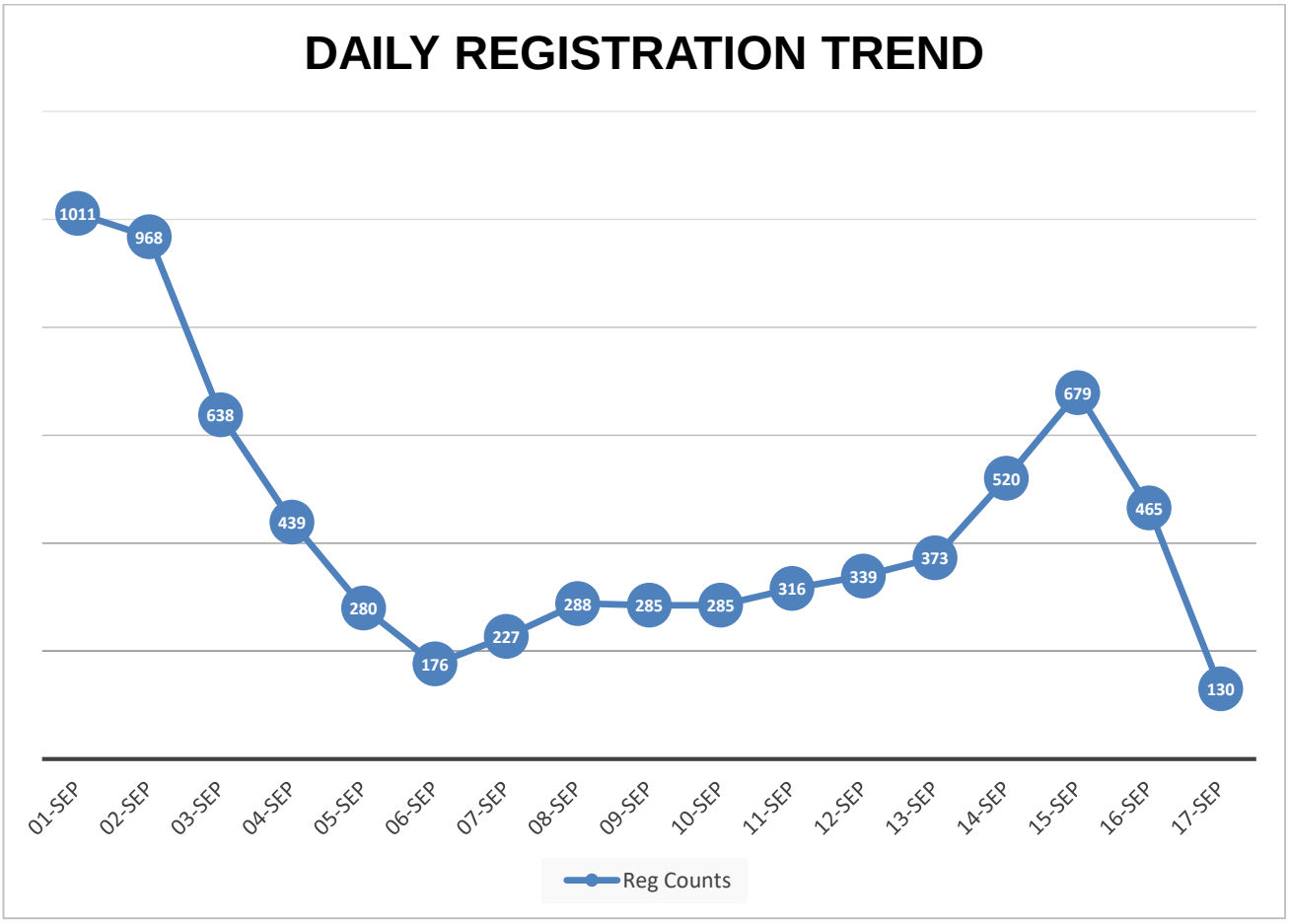
Prior to Bye-Elections held on 14th October, 2018, PP-296 Rajanpur-IV and PP-87 Mianwali-III were declared unopposed by ECP. Furthermore, no voter was registered with I-Voting for PB-40 Khuzdar-III. As a result, Registered Voters (9 in total) from PP-296 Rajanpur-IV and Registered Voters (46 in total) from PP-87 Mianwali-III were excluded from voting through I-Voting bringing the final count of Registered Voters to 7,364 who were eligible to cast a total of 7,461 votes in 35 Constituencies.

## ISSUANCE OF VOTER PASS

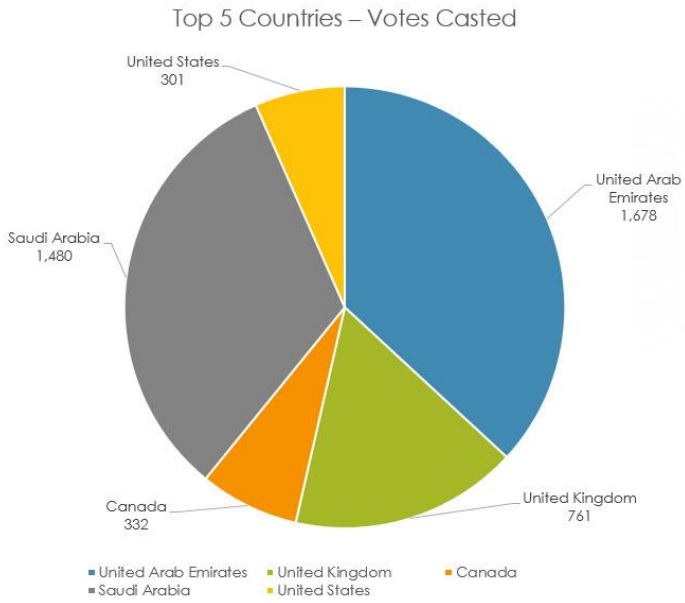
As scheduled, from 10th October 2018 till 14th October 2018, the Election Commission of Pakistan issued Voter Passes to all 7,364 successfully registered voters falling into 35 Constituencies where Bye-Elections were held on 14th October, 2018.

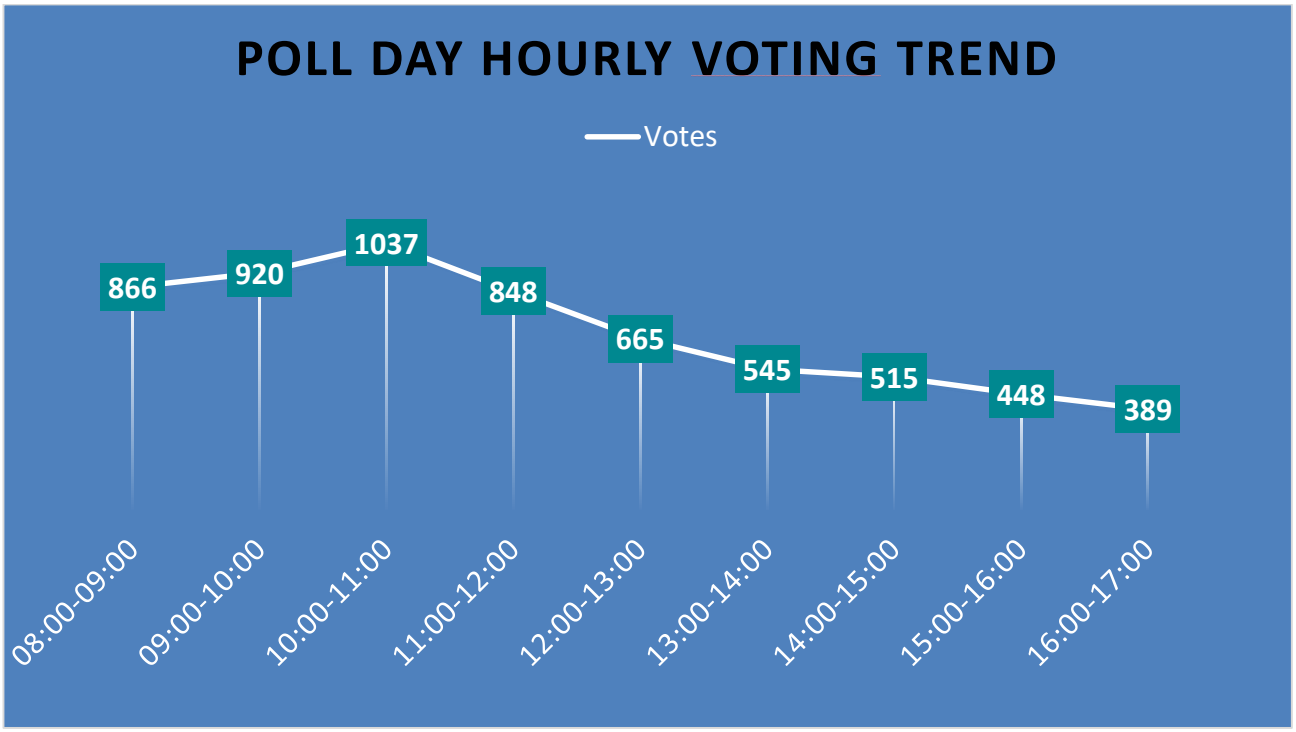
## VOTE CASTING ON ELECTION DAY

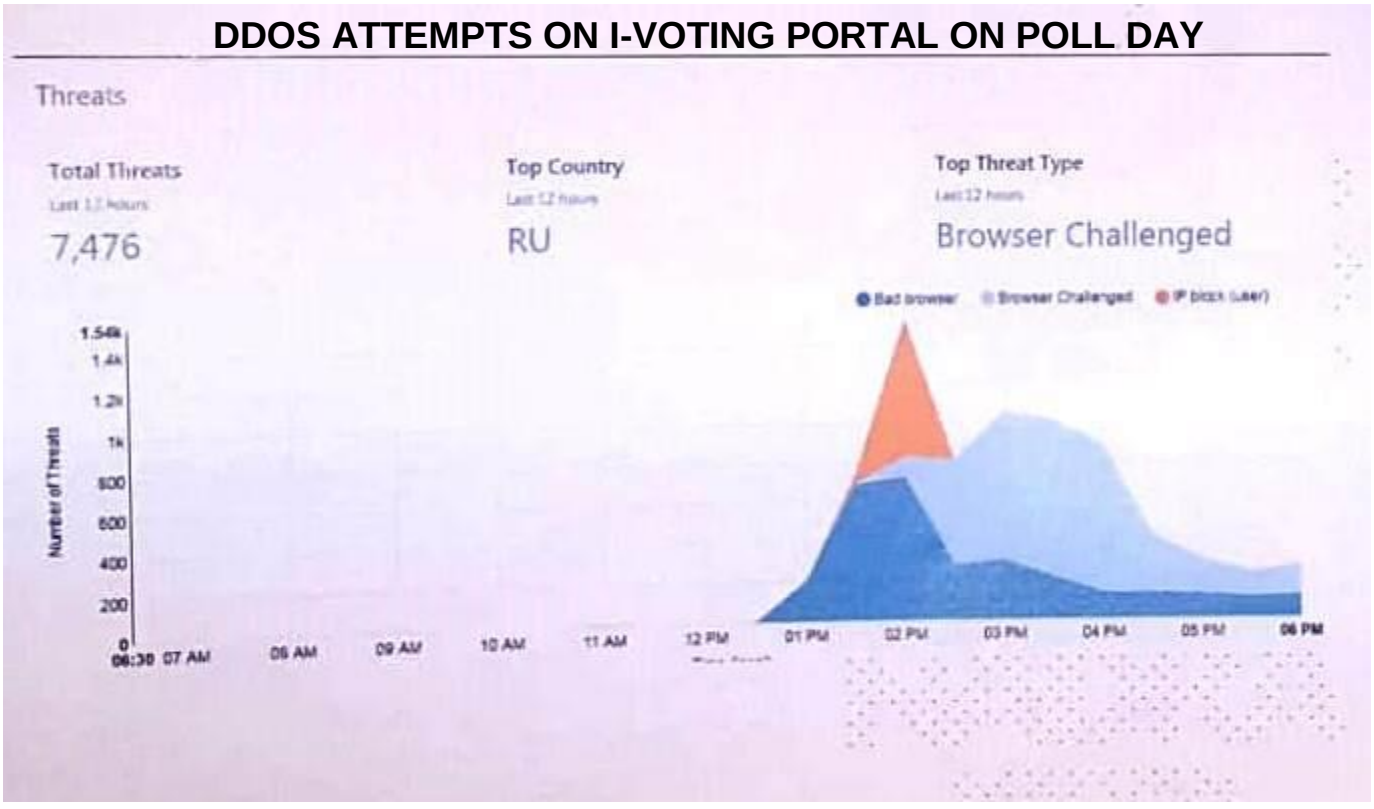
On 14th October, 2018, the Election Day of Bye-Elections, 2018, an overwhelming response was received from the Registered Voters as they wholeheartedly participated in polling through I-Voting. A total of 6,233 votes were casted, out of 7,461 total votes (83.54%) for 35 Constituencies.

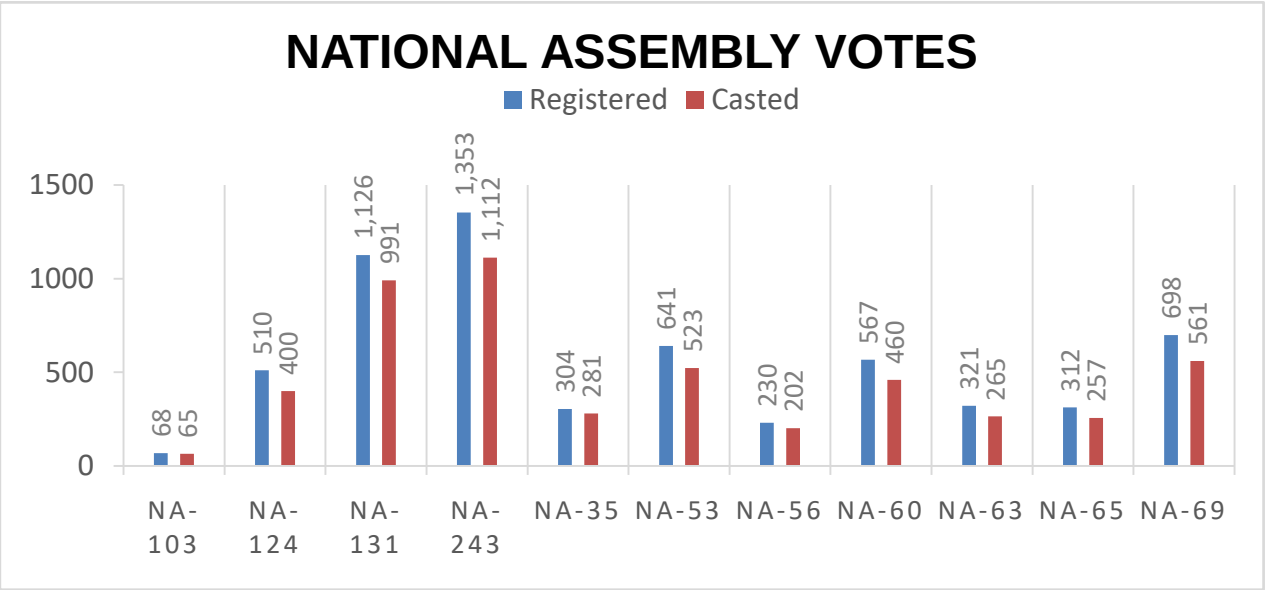


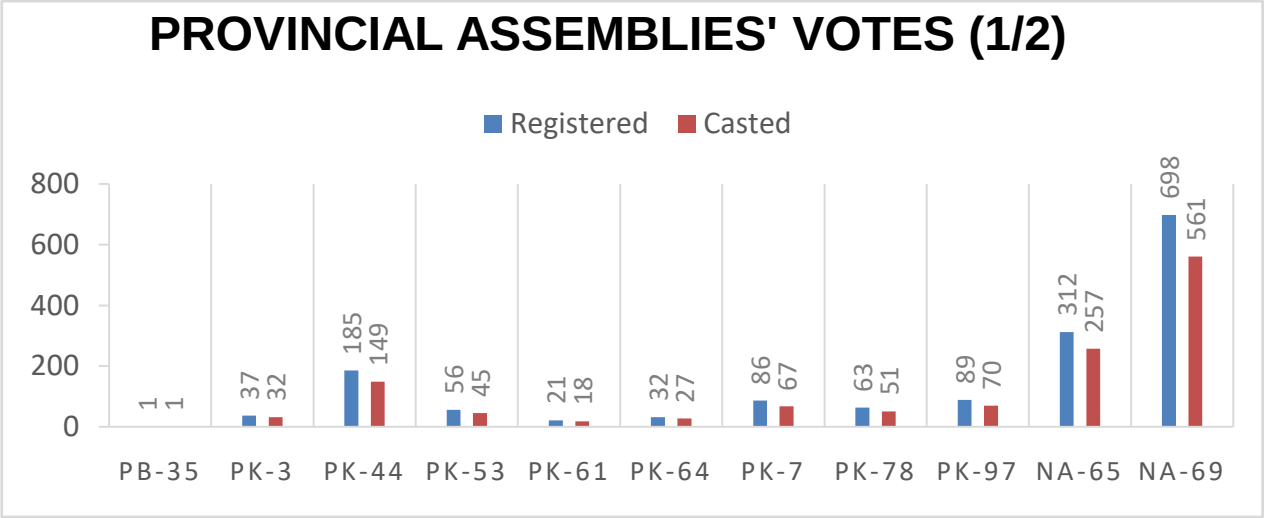

| For Final Voting in 34 Constituencies | Voters | Votes NA + PA |
|---|---|---|
| 1. United Arab Emirates | 1,654 | 1,678 |
| 2. Saudi Arabia | 1,451 | 1,480 |
| 3. United Kingdom | 752 | 761 |
| 4. Canada | 328 | 332 |
| 5. United States | 298 | 301 |

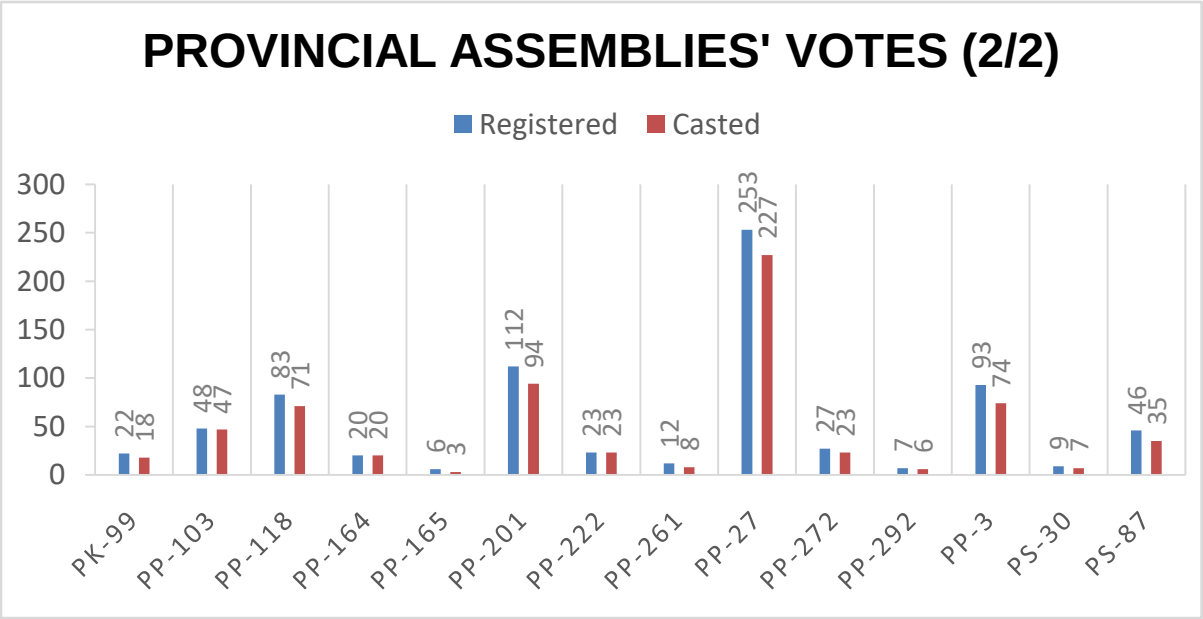



POLL DAY HOURLY VOTING TREND
Votes
866
920
1037
848
665
545
515
448
389
08:00-09:00
09:00-10:00
10:00-11:00
11:00-12:00
12:00-13:00
13:00-14:00
14:00-15:00
15:00-16:00
16:00-17:00


DDOS ATTEMPTS ON I-VOTING PORTAL ON POLL DAY
Threats
Total Threats
7,476
Top Country
RU
Top Threat Type
Browser Challenged
Number of Threats
07 AM
08 AM
09 AM
10 AM
11 AM
12 PM
01 PM
02 PM
03 PM
04 PM
05 PM
06 PM


NATIONAL ASSEMBLY VOTES
Registered
Casted
1500
1000
500
0
68
65
510
400
1,126
991
1,353
1,112
304
281
641
523
230
202
567
460
321
265
312
257
698
561
NA-103
NA-124
NA-131
NA-243
NA-35
NA-53
NA-56
NA-60
NA-63
NA-65
NA-69


PROVINCIAL ASSEMBLIES' VOTES (1/2)
Registered
Casted
800
600
400
200
0
1
1
37
32
185
149
56
45
21
18
32
27
86
67
63
51
89
70
312
257
698
561
PB-35
PK-3
PK-44
PK-53
PK-61
PK-64
PK-7
PK-78
PK-97
NA-65
NA-69


PROVINCIAL ASSEMBLIES' VOTES (2/2)
Registered
Casted
300
250
200
150
100
50
0
22
18
48
47
83
71
20
20
6
3
112
94
23
23
12
8
253
227
27
23
7
6
93
74
9
7
46
35
PK-99
PP-103
PP-118
PP-164
PP-165
PP-201
PP-222
PP-261
PP-27
PP-272
PP-292
PP-3
PS-30
PS-87

## OBSERVATIONS OF ELECTION COMMISSION OF PAKISTAN

***[Technical Efficacy, Secrecy, Security, Operations, Administrative]***

1) What if one does not have a Machine Readable Passport;

2) What, if a Kafeel, especially in UAE/ Saudi context, gets all the computerized passport and NICOPs from his employees/group of employees and does the entire process himself;

3) What is the nature and potential of cyber threat to data in transit over the internet, given the recent reports of cyber attacks during pilot runs. What are the steps taken to mitigate. Is the capability of NADRA better than USA whose system was hacked by Russia;

4) As we were on experimental stage, therefore, the interested parties did not materially interfere merely to put us off track. When the system is finalized and put into practice in toto in the next elections, shall we be able to counter/control cyber attacks;

5) The secrecy of ballot is highly vulnerable and we would be totally compromising it to accommodate a political slogan;

6) The system of voting is so complicated that it shall be definitely exploited to the maximum by interested parties, which would always be there to rigg.

## CHALLENGES

Following challenges were faced during pilot testing of Internet Voting System in bye-elections:-

***[Technical Efficacy, Administrative & Operations]***

- As per I-Voting system set criteria, Machine Readable Passport (MRP) was compulsory for registration process of the voters. It was observed that due to this condition, approximately 15% potential voters of 35 constituencies were deprived from the voting rights. Similarly, dual national having only CNIC were not able to register themselves on the I-Voting System;

***[Technical Efficacy, Secrecy, Security, Operations and Administrative]***

- The I-Voting system was difficult to use for labour class, who are working abroad specially in middle east as well as other parts of the World, not having IT based proficiency and skills as a result, registration process percentage was very low;

***[Technical Efficacy, Operations & Administrative]***

- It was also observed that due to tight Election Schedule, the registration process of overseas voters was opened for very short period i.e. 17 days, which has also contributed in low voter registration turnout;

***[Technical Efficacy, Secrecy, Security, Administrative and Operations]***

- NADRA reported that Distributed Denial of Service (DDOS) attacks was launched on I-Voting website on poll day i.e. 14th October 2018, which was intercepted effectively, however, in future chances of these kind of attacks will always remain there as a potential hacking threat. Similarly, foreign entities can compromises ballot secrecy and potentially even modify ballot contents of voters in an undetected manner;

***[Secrecy, Security, Operations]***

- In case of hacking of voters' email, chances of misuse of voter's ID does also exist;

***[Secrecy, Security, Administrative and Operations]***

- Some incidents were reported that few voters disclosed the secrecy of vote by capturing the screen of Internet Voting portal during voting process and shared the same on social media. In future, these kinds of trend may also spoil the basic concept of election process, that is secrecy of ballot as per Article 226 of the Constitution of the Islamic Republic of Pakistan;

***[Technical Efficacy, Operations and Administrative]***

- During the registration process, it was observed that there was no interactive support/call center was available for overseas voters, where they can raise their queries and questions could be addressed on real-time basis, however, NADRA has introduced an Email based complaint system, which was only meant for only I-Voting portal's registered voters, which was not sufficient to cater the queries and complaints of worldwide overseas voters/general public. Due to this limitation, users/voters faced difficulties for redressel of their complaints and

questions based on general queries. As a result, many complaints were directly responded by ECP Secretariat;

***[Technical Efficacy, Secrecy & Operations]***

- There is no record of the proceedings, hence, no evidence is available in case internet voting changes the result of any constituency and same is challenged through an election petition in that constituency there is no evidence is available of the any activity in such process for paper audit.

***[Technical Efficacy, Secrecy, Security, Operations & Administrative]***

- The recent incident of data theft/hack of banking customers of major local banks in Pakistan created serious data security and privacy concerns resultantly it attracts doubts on all types of (online) electronic transactions. The cyber crime, cyber terrorism and vandalism are the common electronic challenges for any organization in the IT world. This episode was havoc in the electronic banking system of the country, where the all credentials of the customers were leaked and then sold in the Deep Web using Dark Web Technologies by the renowned hackers.

***[Financial feasibility]***

- The pilot project cost is about Rs. 95 million but if it is assumed to think for national roll over then it will cost Rs. 150 million as per NADRA.

## WAY FORWARD

After the completion of first pilot test of Internet Voting for Overseas Pakistanis in bye-elections in 35 constituencies held on 14th October 2018, it is suggested that following recommendations may be considered before continuing pilot testing in future bye-election of any National/Provincial Assemblies constituency to gauge the performance, feasibility and security of I-Voting system:-

- Based on first pilot feedback, some modifications/improvement in I-Voting Software are required to be made like Machine Readable Passport was added in the system as additional security feature during registration process for voters' verification purposes, which causes low voter registration. However, as per law, the Machine Readable Passport is not mandatory for overseas voting registration

like NICOP. It is, therefore, recommended that some other security features may be added like verification through phone number by sending One Time Password (OTP), which is used by most banking systems for secure transactions;

- Ministry of Foreign Affairs, Ministry of Overseas Pakistanis and Overseas Pakistanis Foundation may be requested to extend their support for overseas voters awareness and education programme as well as media campaigns through Embassies and Consulates for maximum participation in I-Voting process;

- NADRA may devise such mechanism that overseas voters' registration process may continue for sufficient period of time, so that voters' education and awareness campaigns may be carried out properly to reach out maximum number of voters spread over different parts of the World;

- For future pilot testing, NADRA may establish an interactive call/complaint center at large scale for redressel of queries of all overseas voters from worldwide during Election Schedule;

- Some necessary reporting features may also be added in I-Voting software like detail forensic record of any particular event may be made available as and when required by the Honourable Election Commission for Audit purpose;

- Security features of the I-Voting System may also be improved based on risks that were identified during the execution of first pilot.

**~*~*~*~*~**

ANNEXURE-A

# FINDINGS AND ASSESSMENT REPORT

# OF

# INTERNET VOTING TASK FORCE (IVTF)

# ON

# VOTING RIGHTS OF OVERSEAS PAKISTANIS

# EXECUTIVE REPORT 2018

***Confidential***

# Table of Contents

# 1 EXECUTIVE SUMMARY

## 1.1 INTRODUCTION

On April 12, 2018, the Honorable Supreme Court of Pakistan convened a historic session (Ref: Const.P.NO.2/20118-SCJ) pertaining to the voting rights of overseas Pakistanis. This session was presided over by Chief Justice of Pakistan, Justice Saqib Nisar, and included members of various political parties, IT experts from Pakistani universities, concerned citizens, and members of the media. On this occasion, NADRA demonstrated iVOTE, an e-voting platform that would allow overseas Pakistanis to cast their votes for the forthcoming General Elections using the Internet.

All parties in attendance strongly affirmed the right to vote for overseas citizens. However, invited IT experts aired concerns about the potential security issues posed by deployment of this system. As a result, on directions of the Supreme Court of Pakistan, the Election Commission of Pakistan constituted a Task Force on April 19, 2018, to undertake a technical audit of the iVOTE platform.[1]

This document presents the views and findings of this Task Force.

## 1.2 IMPLICATIONS

To put Internet Voting in proper context and to highlight the magnitude and gravity of this decision before us, we would like to draw the reader's attention to the following points:

1. Online voting systems have thus far catered to relatively small numbers of voters. If we consider the largest deployments of Internet voting in the world, a mere 70,090 online votes were cast in the Norwegian elections in 2013, 176,491 in the 2015 elections in Estonia, and over 280,000 votes in the state election in New South Wales, Australia. In contrast, iVOTE, if deployed in the forthcoming General Elections, will cater to an estimated more than 6 million overseas voters, and will be the largest ever deployment of Internet voting in the world by far.

2. Leading international cybersecurity professionals have repeatedly voiced serious concerns regarding the security of Internet voting. Researchers have discovered vulnerabilities and launched devastating attacks on such systems (including those deployed in the US, Estonia and Australia) that impacted tens of thousands of votes.[2] These demonstrations have played a determining role in discouraging deployment of Internet voting in several developed countries.

3. In the case of the aforementioned examples, the risk of system failure or mishap has been restricted to relatively small populations and geographical regions. However, in

[1] For details and ToRs of this exercise, please consult the ECP Order of 19 April, 2018, F. No. 6(1)/2011-IT.
[2] Halderman, J. A. (2016). Practical attacks on real-world E-voting. Real-World Electronic Voting: Design, Analysis and Deployment, 145-171.

our case, failure or electoral rigging overseas is not confined to a few seats and can potentially impact each and every constituency in Pakistan, thereby playing a critical role in formation and composition of the next government.

4. Over time Western countries have established strong and resilient mechanisms to investigate and resolve electoral disputes. In comparison, our mechanisms, as evidenced in the aftermath of the General Elections of 2013, are still very fragile. Therefore, electoral improprieties in the overseas voting process (or even the impression of such) can potentially lead to political deadlock and turmoil. To successfully deploy a new technology, we should be cognizant of the relevant social factors.

## 1.3 FINDINGS

Our team undertook a review of iVOTE as per the ECP Order of April 19, 2018 (Ref: F No 6(1)/2011-IT). We identify numerous security vulnerabilities and oversights.

The following is a summary of our most important findings:

1. iVOTE categorically does not provide ballot secrecy as required in Clause 94 of the Elections Act 2017 and Article 226 of the Constitution of the Islamic Republic of Pakistan. This shortcoming is inherent to this particular model of Internet voting systems. Certain territories have explicitly legislated for it: for instance, several states in the US that offer Internet voting require citizens to waive their right to a secret ballot.[3]

2. Casting votes outside a poll-booth environment typically enables vote buying and voter coercion. In our particular case, there is a very real possibility that votes may be bought and sold and coerced overseas in regions where the ECP has no mandate to investigate or prosecute such attempts.

3. We discover that users can easily mount attacks on this system using their web browsers whereby they can cast votes for whichever national and provincial seat they choose, regardless of their constituency. These attacks can be launched with moderate technical ability and can easily be automated to manipulate votes at a large scale.

4. We investigate the possibility of phishing attacks, whereby an attacker creates doubts and confusion in the minds of voters with fake and misleading emails. We successfully sent fake emails addressed from NADRA, with content of our choice, which directed voters to a fake voting website, identical to the iVOTE portal in appearance. These

[3]Orcutt, M. (2016, August 18). Internet Voting Leaves Out a Cornerstone of Democracy: The Secret Ballot. MIT Technology Review.

attacks are exceedingly common and are especially effective against a population, which is not very tech-savvy. The banking sector typically deploys verifiability mechanisms and additional checks to prevent these attacks, but iVOTE has no such mechanism.

5. Distributed Denial of Service (DDos) attacks are a persistent threat on the Internet. NADRA has deployed a leading international filtering solution to protect against these attacks. However, as election security researchers have pointed out recently, this arrangement again compromises ballot secrecy by enabling foreign entities to decrypt and view (and potentially even modify ballot contents of voters in an undetected manner).[4]

6. iVOTE employs certain third-party security components which have been phased out because their security has been demonstrably compromised. These components can be exploited by attackers using freely available tools.

We note that many of these security vulnerabilities are not specific to iVOTE but are inherent to this particular model of Internet voting systems. Therefore, even if the voting system itself has ironclad security, these attacks will still be effective because they do not target the voting system, but instead they focus specifically on the voter's computer and the underlying network, both of which are not under NADRA's control. For this reason, certain territories (such as Estonia) have recently announced that they are abandoning this particular model of Internet voting in favour of a rigorous cryptography-based solution.[5]

Here we list some pertinent observations and concerns regarding iVOTE:

1. No usability studies or tests have been undertaken on iVOTE to ensure ease of use for voters. Ideally such a critical system would go through multiple large scale mock trials for Pakistanis from all walks of life, (especially those with low literacy). This is an extensive and time-consuming process, which may necessitate alterations in the design, which in turn will require further development and security analyses.

2. iVOTE emails are dispatched from an unauthorized email server with the result that emails to voters typically end up in the Spam folder. If these emails are dispatched at high volumes, this may result in wholesale blocking of emails and this can considerably hinder the voting exercise.

3. Certain Internet voting systems provide superior security compared to iVOTE by enabling a measure of redundancy, ballot secrecy, coercion-resistance, and

[4]Culnane, C., Eldridge, M., Essex, A., & Teague, V. (2017, October). Trust Implications of DDoS Protection in Online Elections. In International Joint Conference on Electronic Voting (pp. 127-145). Springer, Cham.
[5]Ummelas O. (2017, July 18) World's Most High-Tech Voting System to Get New Hacking Defenses. Bloomberg

verifiability. For instance, Internet voting systems in Estonia, Norway, and New South Wales were deployed alongside precinct-based paper voting systems. In the event that the Internet voting system failed, citizens in these territories would have been able to vote using paper ballots. Citizens could ensure ballot secrecy and avoid coercion by casting their vote multiple times using different modalities. Moreover, voters could also verify that their votes were correctly recorded in the system via the Internet or telephone. In contrast, iVOTE does not offer any such fail-safe, ballot secrecy, coercion resistance or verifiability features.

4. We note serious governance issues: for instance, we did not find any formal Solution Requirements Specification (SRS) for this project or proper code documentation, which is standard practice when building such systems. We also did not find any formal specification of the Threat model, which was considered when building this system.

5. We did not find any documentation related to key operational processes regarding iVOTE. It has still not been determined which party will administer this system, which premises it will be hosted on, and which personnel will ultimately be responsible for certain critical processes. As a result, at this stage we are unable to assess for certain important security attacks.

6. We anticipate that the monitoring requirements for such a system on Election Day will be considerable. We are not aware of any resources or planning done thus far to provide for this requirement.

7. This lack of planning also poses a considerable security risk in that certain critical security processes are vulnerable to insider attacks, i.e. certain system operators may be in a position to attack the system from within and modify the results. Protection against such attacks requires formulation of security policies, procedural controls, security clearances, etc. which are very intensive and time-consuming processes.

8. Members of the committee observe that even though iVOTE is built using certain mature and well-established technologies, certain others are being replaced by new advanced architectures and technologies. We recommend these should be considered in developing such systems.

We have included remediation measures, wherever possible, in the detailed report.

We would also emphasize here some fundamental limitations of our study. Our committee comprised members with diverse backgrounds, working within a very small-time window, with limited resources, and our analysis is necessarily limited. We did not use specialized hacking tools or mount highly advanced attacks that are more characteristic of cyberwarfare

and attacks undertaken by security agencies. Our report should therefore be considered a preliminary analysis of this system. It is our firm recommendation that iVOTE be subjected to a comprehensive security audit, specifically undertaken by qualified cybersecurity professionals.

## 1.4 RECOMMENDATIONS

Considering all these points, it is this committee's unanimous opinion that deploying Internet voting for overseas Pakistanis in the General Elections of 2018 would be a hasty step with grave consequences. **We do not recommend the deployment of the iVOTE system in its current form for overseas Pakistanis in the forthcoming General Elections of 2018.** However, we do not believe there is cause for pessimism. In our report, we provide suggestions for alternative solutions and long-term strategies to facilitate overseas voters.

Our findings are consistent with those from technical audits conducted on Internet voting systems in the past (such as those deployed in Estonia, New South Wales, and Washington DC). Developers typically approach design these applications as they would build typical commercial or enterprise applications in e-commerce and banking. What is notably missing is a **bottom-up security culture** that is more appropriate to a critical national application such as political elections.

## 1.5 FUTURE DIRECTIONS

Devising a complete alternative mechanism is beyond the scope of this committee, but we have attempted to identify some promising options. Here we present a summary:

1. Ideally new voting systems should be deployed progressively, starting with mock trials, deployment in surveys and non-political elections, followed by small-scale elections, and then scaling up over a period of years. This approach – undertaken by countries like Switzerland and Estonia – has the advantage of identifying vulnerabilities at every step, while at the same time, containing the risk appropriately. This also enables voters to become more familiar with the system and for developers to incorporate improvements in the system. We recommend a similar roadmap be devised for iVOTE along with appropriate milestones at every stage.

2. We recommend that ECP reconsider other remote voting modalities, which are less controversial than Internet voting and have been successfully deployed in many other countries. We note that postal voting is significantly safer than Internet voting in that, even though both modalities compromise ballot secrecy, postal voting is nevertheless not susceptible to hacking attacks which can completely compromise election integrity.

3. Furthermore, embassy voting, while it poses significant logistics challenges and financial constraints, is even safer than postal voting because it preserves ballot

secrecy and protects against coercion. In fact, our strongest recommendation of an alternative option for voting for overseas Pakistanis is to consider deployment of iVOTE in embassies using a closed intranet solution.

We also propose certain general recommendations and long-term strategies:

1. There is a critical shortage of cybersecurity skills and expertise in Pakistan, particularly within the field of election security. We therefore strongly recommend that ECP launch a dedicated and well-funded research and development (R&D) cell with long term and broad ranging objectives. This cell will be specifically tasked with building much-needed technical capacity and skills in this domain, in informing and guiding the public debate on election technology, and in developing secure new technological solutions for elections in Pakistan.

   This effort may be undertaken in partnership with universities and local and international experts. The US government has a strong record in this regard of partnering with leading academics and specialists to develop next-generation voting technologies. Engagements such as these can serve as the model for this R&D cell.

   We understand the ECP has considered such an option various times in the past but has not followed through. Due to this lack of dedicated technical expertise, we witness past mistakes being repeated and no tangible progress on the development of election systems in Pakistan.

2. As part of this R&D cell, we recommend the ECP initiate research and development in revolutionary new models and technologies for secure voting, especially the revolutionary new paradigm of end-to-end (E2E) verifiable voting. E2E voting systems offer cryptographic guarantees of ballot secrecy and election integrity, and these systems are already being trialed in various parts of the world in small-scale binding elections. [6] Most notably, Estonia has announced it is shifting to this new technology. We believe it holds considerable promise for the future, especially in Pakistan.

3. We would urge the ECP to strive towards strengthening electoral dispute resolution mechanisms in Pakistan, such that the deployment of new technological solutions is facilitated in the future.

[6] Ali, S. T., & Murray, J. (2016). An overview of end-to-end verifiable voting systems. *Real-World Electronic Voting: Design, Analysis and Deployment*, 171-218.

## 1.6 CONCLUSION

We hope our report serves as an informative and useful resource in the development of election technology in Pakistan. Internet voting is a controversial issue and we have made every effort to situate this debate on strong technical foundations. Furthermore, we have attempted to focus on one critical element that has been notably missing from the public debate, which is the experience of other countries using this modality. Some of the most technologically advanced countries in the world have either rolled back online voting or have deliberately chosen not to deploy it. In this document, we have highlighted the key features of their arguments and explored their application to our situation.

In conclusion, the members of this committee would like to thank the Election Commission of Pakistan for assisting us in our work. It has been a privilege and an honour to serve the nation in this regard. And we are particularly grateful to NADRA for their kind hospitality, for patiently answering our questions, for providing us timely technical support, and for facilitating this Task Force in all of its efforts.

# 2 INTERNET VOTING TASK FORCE (IVTF) AND OTHER STAKEHOLDERS

## 2.1 IVTF MEMBERS

| S # | Name | Designation/Organization |
|---|---|---|
| 1 | Dr. Muhammad Manshad Satti | CEO, IT Butler, Dubai, U.A.E |
| 2 | Brig ( R ) Sultan Mehmood Satti | M.D, IT Butler, Dubai, U.A.E |
| 3 | Dr. Umer Saif | Chairman, PITB, Lahore |
| 4 | Mr. Sajjad Ghani | Director IT Infrastructure, PITB, Lahore |
| 5 | Mr. Bilal Ibrahim | Program Manager, PITB, Lahore |
| 6 | Mr. Haroon Rasheed | Senior Program Manager, PITB, Lahore |
| 7 | Dr. Syed Taha Ali | Assistant Professor, SEECS NUST, Islamabad |
| 8 | Dr. Shahbaz Khan | M.D, KPIT Board, Peshawar |
| 9 | Mr. M. Asim Jamshed | Director (Projects), KPIT Board, Peshawar |
| 10 | Dr. Rafi us Shan | Chief Cyber Security, KPIT Board, Peshawar |
| 11 | Mr. Zubair Khalid | Sr. Manager, LUMS, Lahore |
| 12 | Mr. M. Qayyum Ahsan | DM Application, LUMS, Lahore |

## 2.2 IVTF AFFILIATE MEMBERS

| S # | Name | Designation/Organization |
|---|---|---|
| 1 | Ms. Hina Binte Haq | Researcher, SEECS NUST |
| 2 | Mr. Bilal Ahmed | Researcher, SEECS NUST |
| 3 | Mr. Zohaib Shaheen | Researcher, SEECS NUST |
| 4 | Mr. Saad Ahmed Khan | SOC System Analyst, IT Butler |
| 5 | Mr. Rafay Baloch | Sr. Manager Info Security Global Eagle Dubai |

## 2.3 NADRA SUPPORTING TEAM

| S # | Name | Designation/Organization |
|---|---|---|
| 1 | Mr. Zulfiqar Ali | D.G (Projects), NADRA |
| 2 | Mr. Waqas Ali | Info. Security, NADRA |
| 3 | Mr. Mohammad Abid | Director (Networks), NADRA |
| 4 | Mr. Junaid Zafar | D.D (Networks), NADRA |
| 5 | Mr. Aftab Ahmed | P.M, NADRA |
| 6 | Mr. Ahmerin Hussain | G.M, Technology, NADRA |
| 7 | Mr. Usman Javed | Head of Software Development, NADRA |
| 8 | Mr. Usman Cheema | Head of R&D, Technology Directorate, NADRA |
| 9 | Mr. Usama Munir | Team Lead Development -iVote System, NADRA |

## 2.4 ECP SUPPORTING TEAM

| S # | Name | Designation/Organization |
|---|---|---|
| 1 | Dr. Akhtar Nazir | Additional Secretary (Admin), ECP |
| 2 | Mr. Muhammad Arshad | Director General(Law), ECP |
| 3 | Mr. Muhammad Khizer Aziz | Director General (Information Technology), ECP |
| 4 | Mr. Qasim Mahmood Khan | Director (Information Technology), ECP |

## 2.5 SCOPE AND TERMS OF REFERENCE (TORS)

1. To get access from NADRA for testing the software code, hardware, network, connectivity, web services, email services, load balancing, security at all levels, database services and its optimization

2. To evaluate the endpoint security protection that detects malicious behavior and prevents malicious files from attacking NADRA networks and systems

3. To Evaluate the Data Security during transmission, applications and web servers commonly using Transport Layer Security (TLS) for encrypted communication

4. To audit the Remote Identity Proofing (RIDP), a process for validating sufficient information that uniquely identifies voter's eligibility (e.g., NICOP, personal demographic information, and other indicators)

5. To evaluate the hosting facility of Overseas Voting Server for Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks on Voting Day or even earlier

6. To assimilate the Man-in-Middle Attacks for ensuring the Data integrity of voting data

7. To identify various types of vulnerabilities and propose optimum solutions

8. To perform comprehensive 'penetration testing' of whole systems

9. To make efforts for compromising the website (www.overseasvoting.gov.pk)

10. To break or hack the iVOTE system and mark its loop-holes

11. To perform load testing activities to check the expected humongous traffic load

12. To give technical recommendations for further enhancing its security

13. To give recommendations on secure use of I-Voting in election activities

14. To submit 3rd party technical audit report to the ECP along with its recommendations for improving or upgrading all aspects of Internet Voting System

15. To give any concrete suggestions, or a proposal for a more secure architecture for I-Voting

# 3 MANAGEMENT INTERVIEWS

In response to complaint assessment of iVOTE application's efficacy, secrecy, and coercion-resistance, it was deemed necessary to conduct informal interviews of Key Stakeholders to ascertain their perspectives and past history of electronic voting systems.

During our meeting with the NADRA chairman, we asked regarding the iVOTE application and its agreed Technical Specification Requirement (TSR) or General Specification Requirement (GSR) from NADRA Management for sign-off process. We found that no formal TSR/GSR has been exchanged or signed off between ECP and NADRA, which reflects the fact that the iVOTE project was hastily instigated to comply with Supreme Court orders.

We also observed that NADRA presented the iVOTE model to Supreme Court with insufficient illustrations of such systems, mostly significantly the fact that no other sovereign state has thus far successfully used such a system at this scale in political elections.

NADRA has undertaken a project to enable over six (06) million overseas voters, and a project of this scope generally takes six to eight months for development. NADRA, under immense pressure, had agreed to develop and test the application in ten (10) weeks' time, which resulted in the lack of software testing processes, no mock elections, and disregarding standard best practices. As a result, IVTF has identified six CRITICAL vulnerabilities and some HIGH categories risks in iVOTE application.

IVTF team has tested the application Vulnerability Assessment (VA) and Penetration Test (PT) from Pakistan and from Overseas (UAE & KSA) and exploited the above weakness and achieved successful penetration in manipulating the data during the voting process. All evidence of our findings (screenshots) are attached in Appendix-A

| S # | Name | Designation/Organization |
|---|---|---|
| 1 | Mr. Babar Yaqoob Fateh Muhammad | Secretary ECP |
| 2 | Mr. Muhammad Khizer Aziz | Director General (IT) ECP |
| 3 | Mr. Usman Y. Mobin | Chairman NADRA |
| 4 | Mr. Zulfiqar Ali | D.G (Projects), NADRA |

During ECP interviews and meetings, we discovered that options for iVOTE and online voting have been evaluated previously during the year 2014 to 2017 but none of those solutions have been fully compliant with voting criteria described in Article 226 of the Constitution of Pakistan and the Election Bill 2017 proposed by the Parliamentary Committee for Electoral Reforms.

It is also worth mentioning here that NADRA and ECP extended us every support, provided us whatever information we requested and assisted the IVTF team during this project.

Likewise, NADRA has facilitated us with a state of the art office environment with a dedicated room, Internet connectivity, on-site visits, and kind hospitality.

# 4 BACKGROUND

Election security is a rich and diverse domain of study and expertise. In this section, we present essential background material on security for Internet voting systems. We start with brief descriptions of the key security properties of voting systems, and we consider how they relate to each other. We describe how Internet voting is distinct from typical Internet applications using the particular example of Internet banking and e-commerce. This is followed by a discussion of how Internet voting faces fundamentally different threats as compared to common Internet applications and how the design of Internet voting systems often fails to take this fact into account. We also briefly consider the legal ramifications of deploying fundamentally new voting technology.

We have attempted to situate this discussion on a firm technical foundation and especially highlight an aspect that is often overlooked in discussion on Internet voting, i.e. the experience of other countries with using this election modality.

## 4.1 SECURITY PROPERTIES

Here, we briefly define various security properties of a voting system.

1. **Voter Eligibility:** The system should only permit eligible voters to cast votes and restrict each voter to one vote.

2. **Ballot Secrecy:** The privacy of the vote is widely recognized as a fundamental human right and is enshrined in Article 21 of the Universal Declaration of Human Rights[7]. The rationale behind this, dating back to ancient Greece and Rome, is that if outside parties become privy to a voter's choice, it opens the door to bribery and intimidation, thereby ultimately corrupting the electoral process. This realization directly motivated the invention of the secret ballot.

   In Pakistan, ballot secrecy for voters is specified as a key requirement in Clause 94 of the Elections Act 2017 and Article 226 of the Constitution of the Islamic Republic of Pakistan.

3. **Coercion Resistance:** The voting system should not allow third parties to force a voter to cast the vote in a certain way. This property directly follows as a result of ballot secrecy.

   Forms of coercion include 'family voting' where one family member casts the votes on behalf of his/her family members or pressurizes them to vote a certain way. Employers may likewise force or incentivize employees to vote for specific candidates. Voters can also choose to sell their votes.

[7] Universal Declaration of Human Rights, 1948

Voter coercion is particularly facilitated in remote voting modalities, such as postal, telephone, or Internet voting, and is a key threat in most of these systems. We quote here renowned cybersecurity expert, Dr. Ross Anderson[8]

*"When you move from voting in person to voting at home (whether by post, by phone or over the internet) it vastly expands the scope for vote buying and coercion, and we've seen this rising steadily in the UK since the 2001 election where postal votes first became a right. All the parties have been caught hustling up the vote in various ways."*

4. **Election Integrity:** The system should instill confidence in voters that the elections have been conducted in a fair manner and that the election results reflect the public will. Typically, election integrity is ensured by **instituting redundancy, transparency,** and **verifiability** measures at key steps in the electoral process. In paper-based election systems, these processes include exit polls, random audits, and opening the tallying process to members of all political parties and citizens. Election integrity is more problematic in electronic and Internet voting systems, as these systems typically do not maintain a paper trail of votes and they are susceptible to large scale hacking.

We list here certain additional non-security properties of voting systems, which are also of critical importance.

1. **Usability:** The system should enable voters to cast their votes easily and effectively.

2. **Accessibility:** The system should provide equal opportunities for access and participation.

3. **Logistics:** This pertains to the cost and ease of setting up a reliable and secure voting system.

Several of the key properties described thus far conflict with each other, giving rise to a variety of technical and legal challenges, which have to be carefully addressed. We consider one of these conflicts next, the clash between vote verifiability and ballot secrecy.

## 4.2 INTERNET VOTING VS. INTERNET BANKING

A very common question, which arises in conversations regarding Internet voting, is that if applications such as banking or commerce can be conducted online, then why not voting? This is a fair question as banking and e-commerce are critical applications and considerable effort is made to secure them. Are the same techniques applicable to Internet voting?

There are two important differences to be considered here: first, online banking and e-commerce systems are vulnerable to cybercrime with attacks costing the economy up to

[8] Nicole Kobie, (2015, March 30) "Why electronic voting isn't secure – but may be safe enough," The Guardian

hundreds of billions of dollars every year. A recent study estimates cybercrime revenue at $1.5 trillion per year and indicates that not only is cybercrime a fast-growing phenomenon but also that cybercriminal outfits may actually be making more money than small and mid-size companies. Banking and e-commerce websites get hacked routinely and the costs of these attacks are typically counted as 'the cost of doing business'.[9]

Second, and most important, the key tools that banks use to fight cybercrime are not applicable to Internet voting. For instance, financial institutions maintain detailed records and audit trails of every transaction. In the case of voting, maintaining audit logs or trails that identify the voter is a direct violation of the secret ballot property. Moreover, Internet voting cannot recover from attacks in the same way that banks can: miscast votes cannot be easily detected or reversed the way banking transactions can. Furthermore, elections are a far more sensitive matter than banking and news of a hacking incident may have a serious negative impact on citizen confidence in elections and long-lasting political repercussions.

In case of an incident, banks and merchants have recovery protocols in place, which include blocking stolen credit cards, reversing irregular transactions, compensating clients for lost funds, etc. Again, these mechanisms do not apply to Internet voting. In the words of election security expert, David Jefferson[10]:

*"Vote fraud is much less manageable than ecommerce fraud. There is no election analog to the natural business practice of "spreading the cost" or "spreading the risk". There is no way to pass on to other voters the "losses" due to illegal ballots cast by ineligible voters or attackers, or to recover votes changed by malicious software. There is no "insurance" that one can buy to cover those losses. There is just no way to compensate for damage done to an election."*

For these reasons, in the election security community, paper is still considered the gold standard when it comes to elections. To quote renowned cybersecurity expert, Bruce Schneier[11]:

*"Today, we conduct our elections on computers. Our registration lists are in computer databases. We vote on computerized voting machines. And our tabulation and reporting is done on computers. We do this for a lot of good reasons, but a side effect is that elections now have all the insecurities inherent in computers. The only way to reliably protect elections from both malice and accident is to use something that is not hackable or unreliable at scale; the best way to do that is to back up as much of the system as possible with paper."*

[9] Glick, B. (2018, Feb. 23) Is cyber security becoming a cost of doing business - to the detriment of our data? ComputerWeekly

[10] Jefferson, D. If I Can Shop and Bank Online, Why Can't I Vote Online? Verified Voting

[11] Schneier, B. (2018, Apr. 18) "American elections are too easy to hack. We must take action now", The Guardian

## 4.3 THE THREAT MODEL

Another crucial distinction between Internet voting and other Internet applications that we overlook in our national discourse is the threat model. Applications such as Internet banking and e-commerce are typically targeted by insiders, hackers or in organized gangs, whereas an Internet voting system used in binding political elections is far more likely to be attacked by foreign governments and intelligence agencies.

Foreign government agencies pose an entirely different class of threat as compared to standard hackers. These organizations typically have unsurpassed resources and capabilities at their disposal. For instance, in 2007 hackers from Russia crippled Estonia's online infrastructure for several days with concentrated Denial of Service attacks that disabled the websites of banks, government ministries, political parties, and media.[12]

These attacks can also be extremely stealthy and powerful and of a magnitude that is sometimes difficult for the layman to even comprehend. We have the example of Skynet, a US NSA operation, specifically deployed in Pakistan.[13] The NSA had actively hacked into Pakistan's communications infrastructure and was surreptitiously engaged in bulk collection of phone metadata of 55 million mobile phone users. This information was then used to identify potential terrorists who could later be targeted via drone strike. This infiltration was undetected for several years and only revealed as part of the Snowden leaks.

Foreign intelligence organizations also possess a wealth of expertise unavailable to the typical hacker. A compelling example is that of a zero-day exploit, i.e. an attack that exploits a previously unknown vulnerability. The Stuxnet worm, designed jointly by the US and Israel, contained four such exploits.[14] Stuxnet infected Iranian nuclear enrichment facilities and destroyed a significant number of centrifuges, launching a new era of cyberwarfare. And since these vulnerabilities are unknown at the time of the attack, there are no defenses against them.

These examples are not isolated cases and hopefully convey the magnitude and gravity of the threat posed by foreign intelligence organizations. These examples particularly apply to Internet voting.

For instance, in 2010, a team from University of Michigan successfully infiltrated a mock Internet voting exercise conducted by the Washington DC Board of Elections and Ethics. Among their findings, the team reported that while they had control of the system, they detected intrusion attempts made by parties in China and Iran.[15]

[12] Tryanor, I. (2007, May 17) Russia accused of unleashing cyberwar to disable Estonia, The Guardian
[13] Naughton, J. (2016, Feb. 21) Death by drone strike, dished out by algorithm, The Guardian
[14] Szoldra, P. (2016, Jul. 7) A new film gives a frightening look at how the US used cyberwarfare to destroy nukes, Business Insider
[15] Wheaton, S. (2018, Oct. 8) Voting Test Falls Victim to Hackers, The New York Times

Similarly, in 2014 Russian hackers attacked Ukraine's presidential election, deleting key parts of the vote tallying software, and came very close to disrupting the election.[16] Russian hackers have also been accused of penetrating voter registration databases in the recent 2016 US elections.

Furthermore, security researchers who successfully attacked the New South Wales Internet voting system (iVOTE), in 2015, successfully demonstrated how zero-day exploits could be used to view and modify votes while they were being cast.[17]

## 4.4 SOFTWARE SECURITY

A last point of note is the poor state of commercial software solutions. We quote election security expert, Dr. Alex Halderman:

*"Real-world internet voting systems tend to be built on top of commercial-off-the- shelf (COTS) software, which, despite the use of the term "commercial," includes most everyday open-source software. Unfortunately, the dominant security practice for COTS developers is still "penetrate and patch." While this approach is suitable for the economic and risk environment of typical home and business users, it is not appropriate for critical security systems, such as voting applications, due to the severe consequences of failure."*

*"Getting web security right is complicated, and small mistakes in the implementation and configuration of web applications can result in total compromise. In this sense, the web is a brittle platform for secure application development. This is illustrated by the vulnerabilities in the Washington, D.C., and New South Wales web-based Internet voting systems… In both cases, vulnerabilities resulting from small oversights—which could have been prevented by changing single lines of code— jeopardized the integrity of election results. Mistakes like these are common in web applications, and they are hard to eradicate because of the multitude of places in the software that they can exist, any one of which might be overlooked."*

This argument particularly applies in our case. In our analysis we discovered that iVOTE relied on a third-party text-based CAPTCHA mechanism that is now retired and demonstrated to be insecure.[18]

## 4.5 VOTING TECHNOLOGY: LEGAL AND POLITICAL ASPECTS

Here we discuss how the introduction of new voting technology interacts with fundamental election security properties, such as ballot secrecy, verifiability, and election integrity, and

[16] Clayton, M. (2014, Jun 17) Ukraine election narrowly avoided 'wanton destruction' from hackers, Christian Science Monitor
[17] Halderman, J., Teague V. (2015, June 5) The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election
[18] Bohannon, J. (2013, Oct. 28) CAPTCHA Busted? AI Company Claims Break of Internet's Favorite Protection System, Wired Insider

the resulting legal and political implications. The examples we discuss also highlight the fact that thus far, advanced technology has mostly fallen short of delivering on election security.

1. **United States:** Over thirty states in the United States allow citizens to cast votes via email, fax, or via the Internet.[19] These options are mostly available to overseas voters and military personnel. However, some twenty states have laws and regulations requiring that voters who vote via the Internet waive their right to a secret ballot. In a further eight states, there is no such legislation but this waiver is still required by election authorities.

   The state of Alaska goes even further and warns voters that their ballot may be corrupted in transit. Voters who visit the voting website are shown a disclaimer from the State Division of Elections[20]: *"When returning the ballot through the secure online delivery system, you are voluntarily waving [sic] your right to a secret ballot and are assuming the risk that a faulty transmission may occur."*

   Alaska has since announced it is suspending its Internet voting program over fears of Russian hacking.[21]

2. **Germany:** For instance, in Germany in 2009, the country's electronic voting program was rolled back after concerned citizens mounted a legal challenge in court, arguing that the average voter could not verify the inner workings of these machines and therefore needed to place "blind faith" in the technology. In its ruling, the Federal Constitutional Court of Germany stated[22]: *"The very wide-reaching effect of possible errors of the voting machines or of deliberate electoral fraud make special precautions necessary in order to safeguard the principle of the public nature of elections."*

   The ruling concludes with: *"In a republic, elections are a matter for the entire people and a joint concern of all citizens. Consequently, the monitoring of the election procedure must also be a matter for and a task of the citizen. Each citizen must be able to comprehend and verify the central steps in the elections."*

3. **Poland:** In December, 2014, Poland's electronic voting system suffered major technical glitches during local elections, delaying results, and leading to widely unexpected outcomes. An estimated 60,000 people marched in protest, including

[19] Orcutt, M. (2016, Aug. 18) Internet Voting Leaves Out a Cornerstone of Democracy: The Secret Ballot MIT Technology Review
[20] Horwitz, S. (2016, May 17) More than 30 states offer online voting, but experts warn it isn't secure, The Washington Post
[21] Juneau Empire, (2018, Feb. 21) To boost election security, Alaska suspends electronic absentee program, Juneau Empire
[22] NDI, The Constitutionality of Electronic Voting in Germany

extremist nationalist groups. Polish courts were flooded with more than a thousand legal challenges contesting election results.

## 4.6 CONCLUSION

Hopefully this discussion thus far demonstrates to the reader why Internet voting is recognized by security experts to be a controversial and risky undertaking. We have described the security properties of voting systems and discussed how they fundamentally differ from those of typical Internet applications. We have also highlighted how the threat model is different and why this is a critical factor that is unfortunately often overlooked in the national dialogue.

We have further summarized findings from attacks on three key Internet voting systems (Washington DC, Estonia, and New South Wales) in Appendix B. It also summarizes key concerns raised in other countries regarding the implementation of Internet voting. The primary issues that other countries have wrestled with were the same security concerns that we raise in this report.

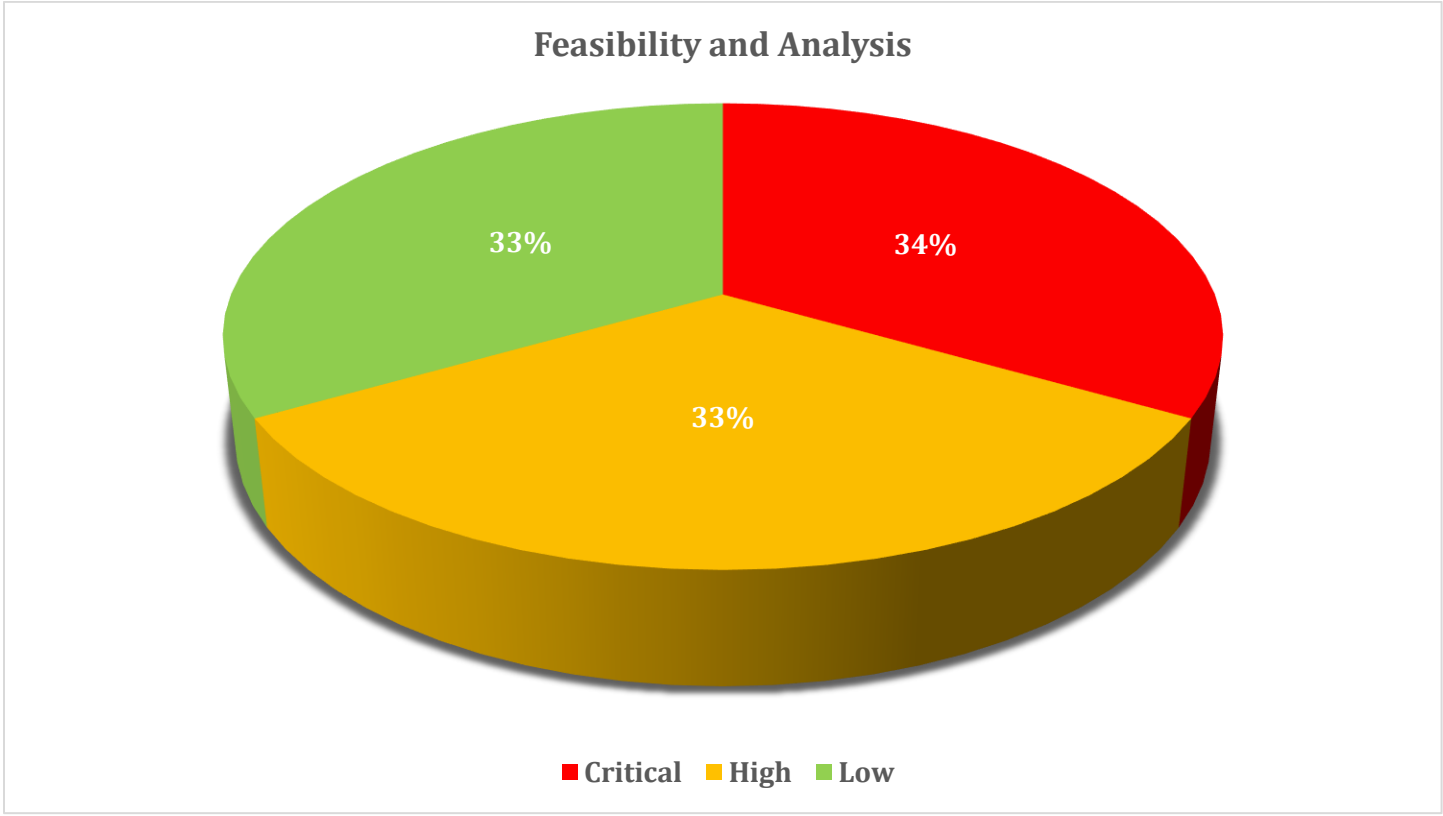
In these cases, researchers were able to exploit very minor flaws in the systems to completely compromise the elections. In the case of the Washington DC Internet voting system, the error was as trivial as using single quotation marks instead of double quotation marks at one point in the code.

We would therefore urge all stakeholders to exercise extreme caution in approaching the question of Internet voting.

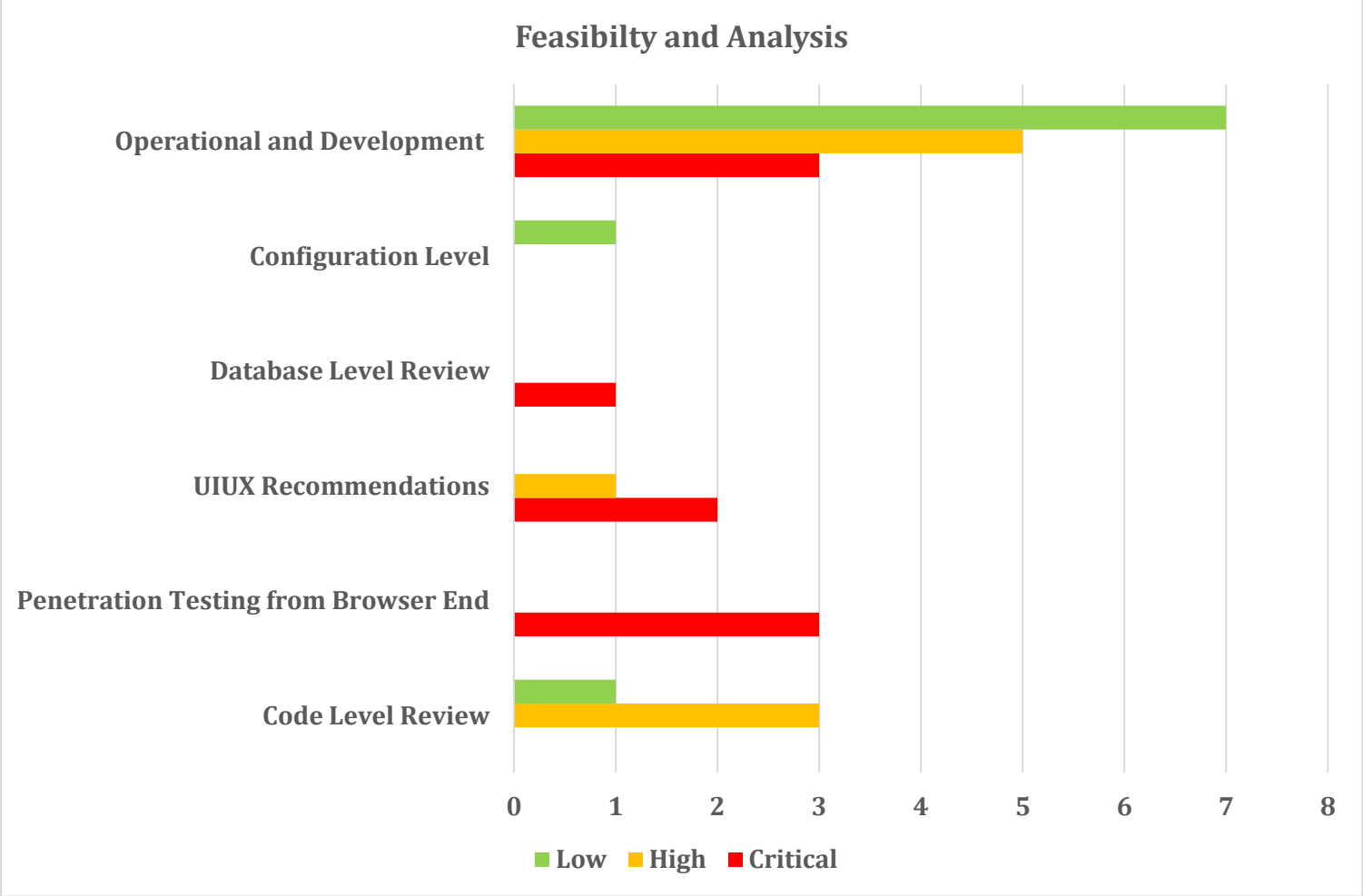
# 5 FEASIBILITY AND ANALYSIS

This section of the report is composed of following areas, each addressed in detail below:

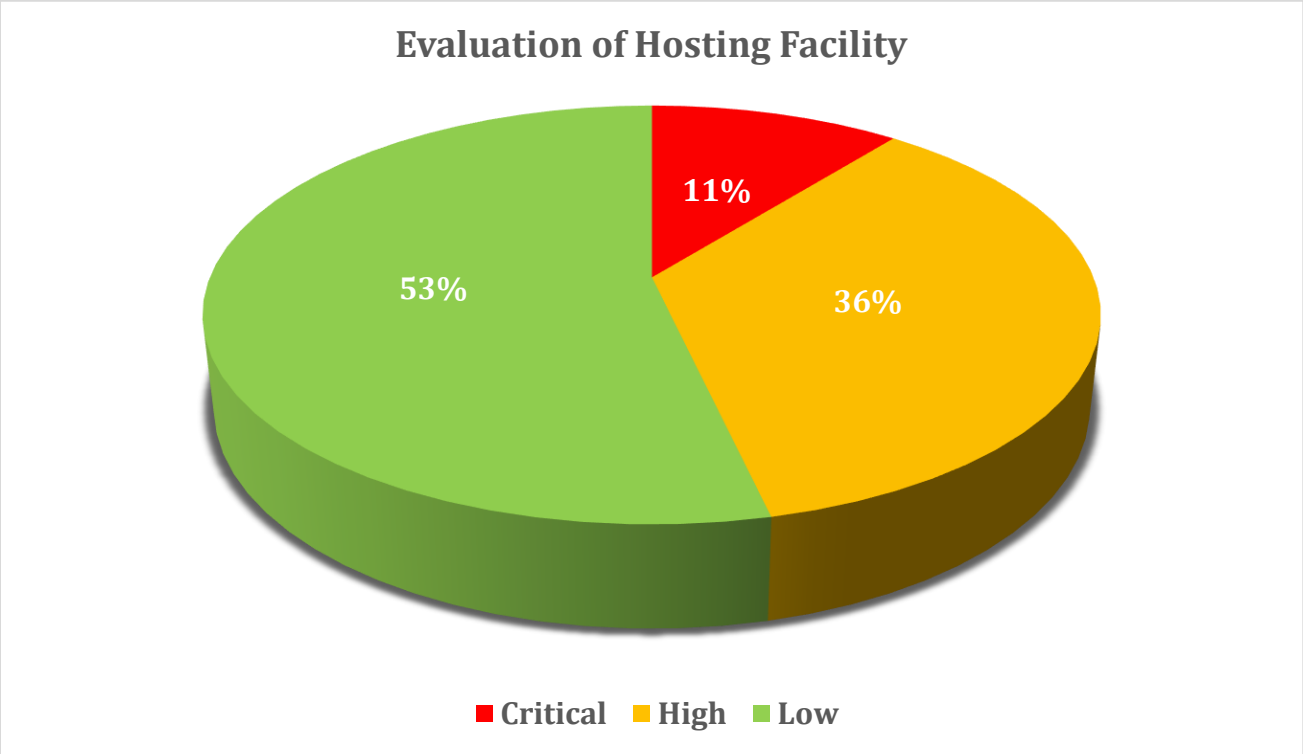
1. Code Level Review
2. Penetration Testing from Browser End
3. UIUX Recommendations
4. Database Level Review
5. Configuration Level
6. Operational and Development



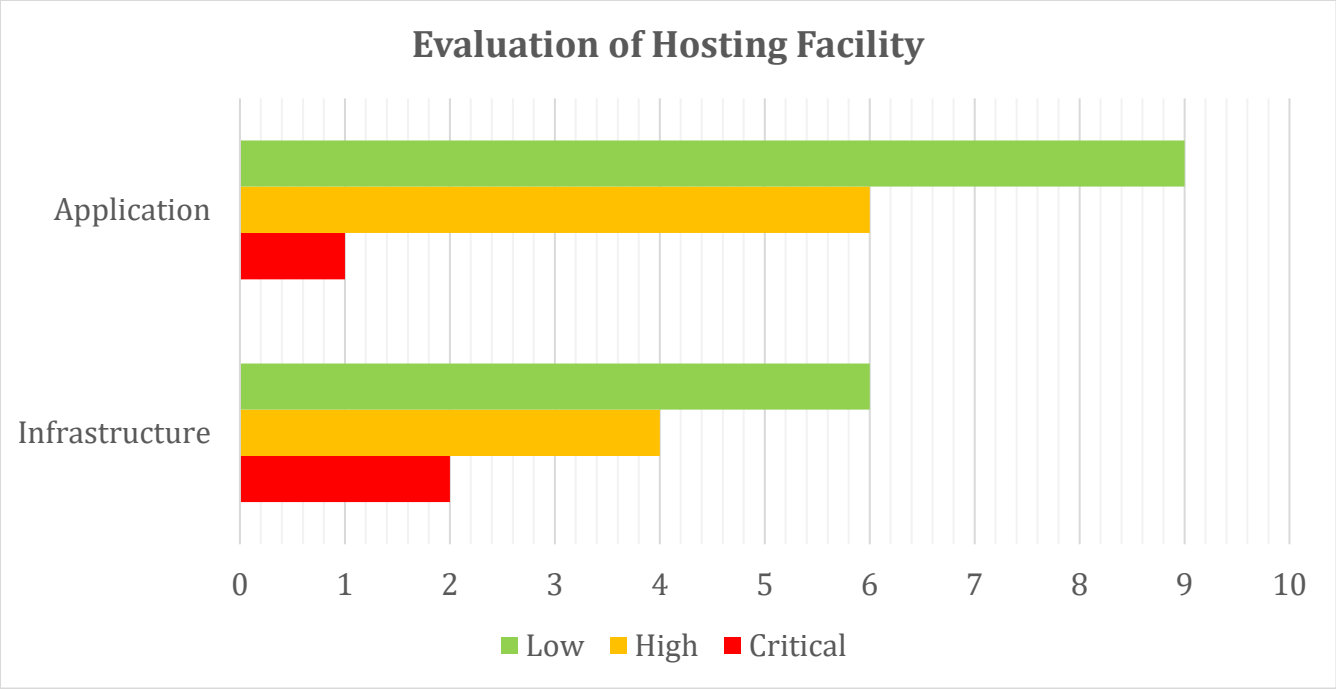

| Sr No | Category | Critical | High | Low |
|---|---|---|---|---|
| 1 | Code Level Review | 0 | 3 | 1 |
| 2 | Penetration Testing from Browser End | 3 | 0 | 0 |
| 3 | UIUX Recommendations | 2 | 1 | 0 |
| 4 | Database Level Review | 1 | 0 | 0 |
| 5 | Configuration Level | 0 | 0 | 1 |
| 6 | Operational and Development | 3 | 5 | 7 |
| | **Total** | 9 | 9 | 9 |


Feasibilty and Analysis
Operational and Development
Configuration Level
Database Level Review
UIUX Recommendations
Penetration Testing from Browser End
Code Level Review
0
1
2
3
4
5
6
7
8
Low
High
Critical

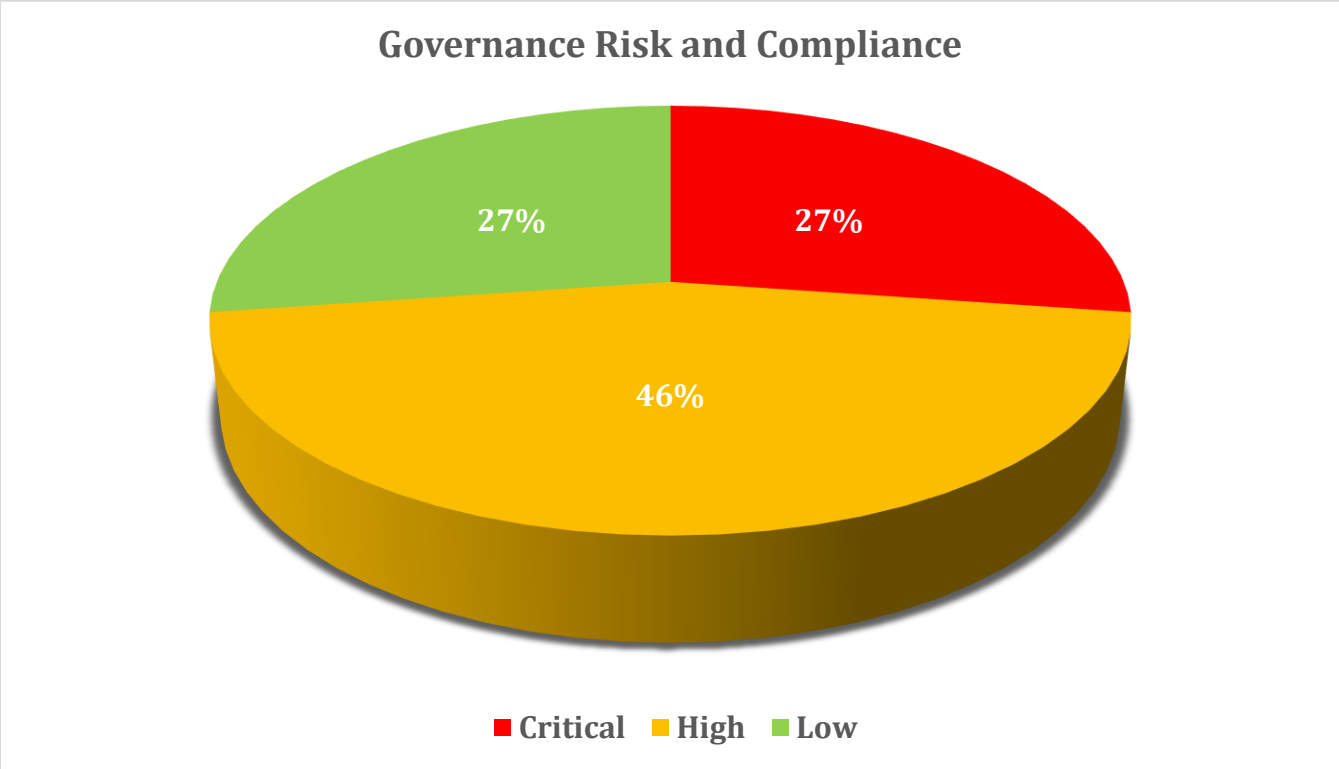
# 6 Evaluation of Hosting Facility




| Sr No | Category | Critical | High | Low |
|---|---|---|---|---|
| 1 | Infrastructure | 2 | 4 | 6 |
| 2 | Application | 1 | 6 | 9 |
| | **Total** | 3 | 10 | 15 |


Evaluation of Hosting Facility
Application
Infrastructure
0
1
2
3
4
5
6
7
8
9
10
Low
High
Critical

# 7 GOVERNANCE, RISK AND COMPLIANCE



# 8 THE WAY FORWARD

In this section, we would like to present our humble recommendations on the way forward. We do not believe there is cause for pessimism in this endeavor. Technology has made great strides recently, especially in election technology, and we anticipate that Internet voting will be a reality in the near future.

First, we present our recommendations for Internet voting. This is followed by a consideration of other remote voting modalities such as postal and embassy voting. We believe that iVOTE, deployed in an embassy-voting scenario, may be a workable technological solution for overseas Pakistanis to vote in the short term.

We then present long-term recommendations, namely that ECP invest wholeheartedly in a Research and Development cell to investigate new cutting-edge election technologies (especially end-to-end verifiable voting) and to educate and guide stakeholders on technological questions.

## 8.1 RECOMMENDATIONS FOR INTERNET VOTING

We recommend that Internet voting, if needed, be deployed in a piecemeal organic manner[23] starting with multiple small non-political elections (e.g. trade organization, bar councils, engineering bodies, etc.), followed by small-scale political elections (intra-party elections, local government polls, by-elections), and slowly expand in scope.

This strategy allows for review and further improvement at every stage in terms of usability and security. The electorate also gets a chance to adjust to this new system and provide valuable feedback. Verifiability measures could be incorporated piecemeal at different stages of the election process. The technical challenges and threat model for deploying such a system also become clear and system administrators develop valuable experience in the process.

Additionally, in the event of technical glitches, hacks, or system failure, the political risk is proportionately restricted. Furthermore, if there are legal challenges to this system (as have been observed in several countries including Germany, India, and Poland), then they can be addressed in a timely manner without wasting resources on a very large deployment.

We would also strongly recommend periodic security audits of this Internet voting system as well as regular sponsored hackathons and bug bounties (similar to those conducted in India[24] and at DEFCON[25]) where hackers are invited to attack the system for monetary reward.

[23] Ali, T. (2015, May 21) How (not) to deploy an electronic voting system, Express Tribune
[24] Bhatnagar, G. V. (2017, May 21) Election Commission Says EVM Hackathon to Begin From June 3, The Wire
[25] Newman, H. L. (2017, Jan. 8) To fix voting machines, hackers tear them apart, Wired

We suggest that all stakeholders contribute to a roadmap for a phased deployment of Internet voting along the lines that we have suggested with appropriate milestones and KPIs to be met at every stage.

## 8.2 ALTERNATIVE REMOTE VOTING MODALITIES

1. **Postal Voting:** Postal voting also suffers from a critical weakness of remote voting paradigms in that ballot secrecy and coercion resistance cannot be ensured. Voters may pressure family members to vote a certain way, votes may be bought and sold in secret, and employers may use incentives or intimidation techniques to force votes for candidates of their choice. For this reason, several countries, including Austria and Germany, require postal voters to sign an explicit disclaimer, where they commit to casting their vote in an unobserved and secret manner.

   However, postal voting has one fundamental security advantage over Internet voting: coercion and rigging efforts on postal ballots are classed as 'retail' attacks which require physical effort and coordination and are considerably difficult to mount on a very large scale. On the other hand, Internet voting systems enable 'wholesale' rigging, i.e. tens of thousands of votes may be altered in a single successful hack. In essence, Internet voting carries a far greater threat to election integrity than postal voting. Furthermore, unlike Internet voting, postal voting has been successfully employed in dozens of countries to date and its risks and methodology are well understood.

   For these reasons, we conclude that postal voting, although it bears heavier logistics and financial costs, is a considerably more secure option than Internet voting. We understand that ECP has conducted mock trials of postal voting in the past without much success. We would recommend ECP consider revisiting this modality as a short-term solution to enable overseas Pakistanis to vote.

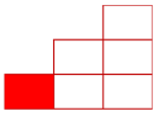
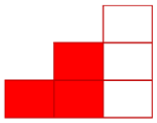
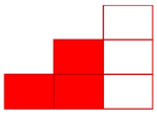
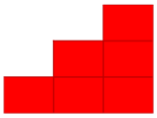
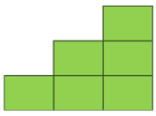
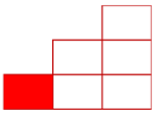
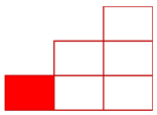
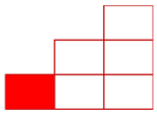
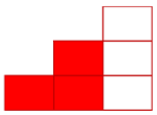
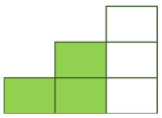
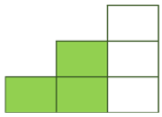
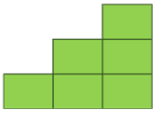
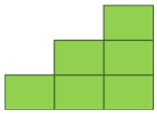
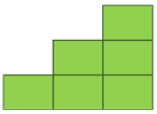
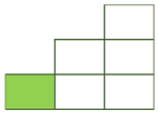
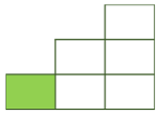
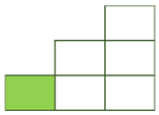
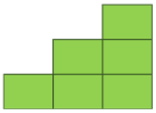
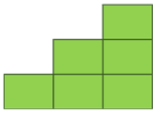
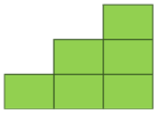
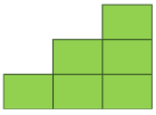
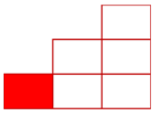
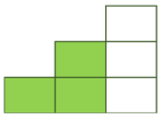
2. **Embassy Voting:** Another desirable modality for remote voting is the embassy-voting paradigm, where voters cast votes in person at the nearest consulates and embassies. This bears significant logistics and financial costs than postal ballots but offers the strongest security of all remote voting paradigms. The embassy environment serves as a makeshift precinct or polling booth, which automatically protects ballot secrecy and prevents voter coercion.
   There is also significant precedent for embassy voting from the examples of other countries. Election security specialists have also recommended it in certain cases specifically as a more secure alternative to Internet voting.[26]

[26] Jefferson. D, (2004, Jan. 5) A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)

In fact, it is even possible to reduce costs by deploying an online voting system on consoles in embassies over a closed network (Intranet), which is not accessible via the public Internet. This protects the system from online hackers and reduces reliance on foreign entities (such as web-based filters e.g. Cloudflare).

We believe this is the most technically secure option to be considered for forthcoming elections. However, as we noted earlier, this modality has various political, financial, and logistics aspects, the study of which is beyond the scope and expertise of this committee. We therefore recommend that the concerned parties undertake a feasibility study of embassy voting for overseas voting.

A summary comparison chart of all three remote voting modalities (postal voting, embassy voting, and Internet voting) is provided below: -

| System | Voter Eligibility | Ballot Secrecy | Coercion Resistance | Election Integrity | Logistics | Usability |
|---|---|---|---|---|---|---|
| Internet Voting |  |  |  |  |  |  |
| Postal Ballots |  |  |  |  |  |  |
| Embassy Voting |  |  |  |  |  |  |
| End to End Verifiable Voting |  |  |  |  |  |  |


## 8.3 Long-term Strategy: Research and Development (R&D)

We urgently recommend that ECP institute a dedicated cell to research and develop cutting edge election technologies as well as provide informed and timely technical expertise to stakeholders in the electoral process. We find these two factors to be critical shortcomings in our national dialogue regarding voting technology. We understand the ECP itself has weighed this option over the past few years but has yet to give it a green light. A dedicated cell that is staffed with experts, with funded resources, a wide-ranging scope, and a long-

term vision will hopefully rectify this deficiency and provide sound advice on future decisions.

There is strong precedent for this step. In the wake of the infamous US elections of 2000, as part of the Help America Vote Act, the US government directly engaged with academics from top American universities and cybersecurity specialists and activists to fund think tanks, research groups, and local conferences which led to significant breakthroughs in the development of election technology. Electoral bodies in other countries also directly fund research and development in new election technology.

Among its first tasks, we would strongly recommend that this R&D cell investigate the use of end-to-end (E2E) verifiable voting technology for potential deployment. This is a revolutionary new paradigm for secure elections that has emerged over the last decade where voters and election officials alike can verify various steps of the election using cryptographic guarantees without compromising ballot secrecy.[27] This technology is being developed and is being actively promoted by some of the most renowned cryptographers and security specialists in the world.

Developed countries worldwide have recognized the revolutionary potential of this new development. E2E voting systems have been trialed in various pilot projects and non-political elections and are now being deployed in binding political elections on a small scale (for instance, in intraparty elections in Israel, in mayoral elections in Maryland, US, in state elections in Victoria, Australia, and at the county level in gubernatorial elections in Texas). Electoral experts in Switzerland and Canada have recommended this new technology be explored for use in forthcoming elections. Most notably, Estonia, on the recommendation of security experts and the Organization for Security and Cooperation in Europe, has announced that it is transitioning to E2E technology, referring to it as the 'Holy Grail' of electronic voting.[28]

Furthermore, the blockchain also presents considerable opportunity for building reliability and trust in the voting infrastructure. Sierra Leone made headlines recently when observers demonstrated how votes cast in the recent presidential election could be stored on a blockchain-based platform[29]. Russia has recently launched a blockchain-based system for voting on municipal initiatives[30] and for preserving exit poll results in recent Presidential

[27] Ali, S. T., & Murray, J. (2016). An overview of end-to-end verifiable voting systems. *Real-World Electronic Voting: Design, Analysis and Deployment*, 171-218.
[28] Ummelas, O. (2017, July 18) World's Most High-Tech Voting System to Get New Hacking Defenses. Bloomberg
[29] Zuckerman, M. J. (2018, Mar. 8), Sierra Leone Uses Blockchain To Track Election Results, Swiss Company Provides Expertise. CoinTelegraph
[30] Castillo, M. (2018, Feb. 21) Russia Is Leading the Push for Blockchain Democracy. CoinDesk

elections[31]. Moreover, researchers have also successfully demonstrated E2E verifiable voting systems, which are powered by the blockchain.[32]

As these new developments indicate, there is a bright and exciting future ahead for electronic and Internet voting technologies. The formation of a cell that is empowered and exclusively dedicated to research and development in these domains would potentially save us considerable time in updating our technical base, reduce our reliance on foreign expertise, develop indigenous and trustworthy solutions, and provide non-partisan, informed and valuable guidance on the way forward.

We strongly urge action on this R&D recommendation. We urge all stakeholders not to overlook or minimize the importance of informed technical research and expertise as has been done multiple times in the past, and which has resulted in this current political deadlock and continues to deprive our citizens of contributing to our democracy.

***** Report Ends Here *****

[31] Suberg, W. (2018, Mar. 6) Russia: Blockchain Will Be Used To Protect 2018 Presidential Exit Poll Data. CoinTelegraph

[32] Castor, A. (2017, Apr. 6) An Ethereum Voting Scheme That Doesn't Give Away Your Vote. CoinDesk

ANNEXURE-B

IN THE SUPREME COURT OF PAKISTAN
(ORIGINAL JURISDICTION)

PRESENT: MR. JUSTICE MIAN SAQIB NISAR, HCJ
MR. JUSTICE UMAR ATA BANDIAL
MR. JUSTICE IJAZ UL AHSAN

CONSTITUTION PETITIONS NO.74 TO 79 OF 2015, 49 TO 56 OF 2016 AND 2 OF 2018 AND CIVIL MISC. APPLICATIONS NO.4292 OF 2017 AND 162 OF 2018
(Under Article 184 of the Constitution)

| | |
|---|---|
| Dr. Farhat Javed Siddique | In Const.P.74/2015 |
| Mujahid Ali Khan | In Const.P.75/2015 |
| Zakir Hussain Naseem | In Const.P.76/2015 |
| Muhammad Zakir Ali Siddiqui | In Const.P.77/2015 |
| Muhammad Asif Chaudhry | In Const.P.78/2015 |
| Solicitor Muhammad Dawood Ghaznavi | In Const.P.79/2015 |
| Kiran Zar | In Const.P.49/2016 |
| Tauheed Ahmed Khan | In Const.P.50/2016 |
| Ghazala Kanwal Asim | In Const.P.51/2016 |
| Asif Malik | In Const.P.52/2016 |
| Junaid Bari Dar | In Const.P.53/2016 |
| Owais Fareed Pirzada | In Const.P.54/2016 |
| Shahryar Jahangir | In Const.P.55/2016 |
| Dure Shehwar Hanif | In Const.P.56/2016 |
| Imran Khan and others | In Const.P.2/2018 |
| Impleadment application by Dr. Arif Alvi | In C.M.A.4292/2017 |
| Impleadment application by Imran Khan Niazi etc. | In C.M.A.162/2018 |

...Petitioner(s)

VERSUS

Government of Pakistan etc.

...Respondent(s)
(In all cases)

For the petitioner(s): Mr. Anwar Mansoor Khan, Sr. ASC
Mr. Faisal Fareed Hussain, ASC
**(In Const.P.2/2018)**

Syed Rifaqat Hussain Shah, AOR
**(In Const.P.74-78/15, 49-56 of 2016)**

Solicitor Mr. Daud Ghaznavi, Petitioner in person in Const.P.79/15)

For the respondent(s)/on notice: Mr. Khalid Jawed Khan, Attorney General for Pakistan.
Syed Nayyar Abbas Rizvi, Addl. Attorney General assisted by Barrister Asad Rahim
Mr. Zikriya Sheikh, DAG

For ECP: Mr. Babar Yaqoob Fateh, Secy. ECP
Mr. M. Arshad, D.G. Law

ATTESTED

Court Associate
Supreme Court of Pakistan
Islamabad

For NADRA: Mr. Usman Yousaf Mobeen, Chairman.
Mr. Zulfiqar Ali, D.G. Projects
Mr. Saqib Jamal, Director, Legal
Mr. Umar Ali A.D. Legal

Dates of hearing: 15.8.2018 (Islamabad) & 17.8.2018 (Lahore)

ORDER

MIAN SAQIB NISAR CJ.- The present petitions were filed by, *inter alia*, certain Overseas Pakistanis prior to the General Elections held on 25.07.2018 with the prayer that they *(Overseas Pakistanis)* be entitled to vote in the General as well as Local Bodies Elections. Pursuant to the order dated 29.01.2018 whereby this Court directed the National Database & Registration Authority *(NADRA)* with the assistance of the Election Commission of Pakistan *(ECP)* to develop a system to provide Overseas Pakistanis with an effective right to vote, an extensive exercise was undertaken. As a result Overseas Voting Solution (Internet Voting) *(i-voting)* was developed. Various presentations were given to this Court to seek validation of the said system. A third party technical audit of the I-voting system was also sought and a report was produced in this regard. While there were certain technical and security apprehensions about allowing Overseas Pakistanis to vote via the internet, the said report was generally positive and encouraging. Be that as it may, in order to ensure that no disruption of any kind was caused to the General Elections 2018, particularly by an overseas voting mechanism which had never been tried or tested before, this matter was postponed to after the said elections. The instant matter has now been revived by this Court.

2. Learned counsel for the petitioners argued that on account of the provisions of Section 94 of the Election Act, 2017 *(the Act)*, it is obligatory for ECP to enable Overseas Pakistanis to exercise their right to vote. It can discharge such obligation by framing the necessary rules under Section 239 of the Act. In response, ECP filed its para-wise comments along with the proposed rules for enabling Overseas

ATTESTED

Court Associate
Supreme Court of Pakistan
Islamabad

Pakistanis to cast their votes through internet. The learned Additional Attorney General for Pakistan has candidly stated that the right to vote of Overseas Pakistanis is enshrined in Article 17 of the Constitution of the Islamic Republic of Pakistan, 1973 *(the Constitution)*. It has been spelt out very clearly in the judgment of this Court reported as **Ch. Nasir Iqbal and others Vs. Federation of Pakistan thr. Secy. Law and others (PLD 2014 SC 72)**. According to him, it is only an appropriate mechanism system and procedure which needs to be put in place by ECP in exercise of its rule making power to determine how this right to vote shall be exercised in practical terms.

3. There are no two opinions about the fact that a citizen's right to vote is sacrosanct and paramount. Article 17 of the Constitution reads as under:-

> *"17. **Freedom of association.** (1) Every citizen shall have the right to form associations or unions, subject to any reasonable restrictions imposed by law in the interest of sovereignty or integrity of Pakistan, public order or morality.*
>
> *(2) Every citizen, not being in the service of Pakistan, shall have the right to form or be a member of a political party, subject to any reasonable restrictions imposed by law in the interest of the sovereignty or integrity of Pakistan and such law shall provide that where the Federal Government declares that any political party has been formed or is operating in a manner prejudicial to the sovereignty or integrity of Pakistan, the Federal Government shall, within fifteen days of such declaration, refer the matter to the Supreme Court whose decision on such reference shall be final.*
>
> *(3) Every political party shall account for the source of its funds in accordance with law."*

ATTESTED

Court Associate
Supreme Court of Pakistan
Islamabad

In **Ch. Nasir Iqbal**'s case *(supra)* this Court interpreted Article 17 *ibid* and held that:-

> *"6. Under Article 17 of the Constitution every citizen has the right to vote to participate in the governance of the country through their chosen representatives...*
>
> *8. It is to be noted that there is no distinction between the citizens living within Pakistan or outside the country, with regard to the right to vote in terms of the Article 17 of the Constitution...It warrants to mention that the right to vote has not been denied to the overseas Pakistanis, who are as much important as those living inside the country, but only the facilities to vote, which provides the sense of ownership and participation in the governance of the country, has not been extended to them...*
>
> *9. It must be clarified here that the overseas Pakistanis, as noted hereinabove, enjoy the right to participate in the election process in terms of Article 17 of the Constitution being dignified citizens of the country, though residing outside its territory, as such they cannot be denied the same rights on technical grounds, i.e. logistic arrangements made outside the country for casting their votes.*
>
> *13. ...Article 17 of the Constitution continues to insist upon the Federal Government to extend the facility of voting to overseas Pakistani in the election of the Parliament as well as Local Bodies."*
>
> *[Emphasis supplied]*

It is pertinent to note that after the aforementioned judgment was passed, no concrete steps were taken to actualize this right to vote for Overseas Pakistanis and enable them to participate in the electoral process while working/residing outside the territorial boundaries of Pakistan. However, subsequently the Act was promulgated on

ATTESTED

Court Associate
Supreme Court of Pakistan
Islamabad

02.10.2017. Section 94 whereof deals with voting by Overseas Pakistanis as follows:-

> *"94. Voting by Overseas Pakistanis.—(1) The Commission may conduct pilot projects for voting by Overseas Pakistanis in bye-elections to ascertain the technical efficacy, secrecy, security and financial feasibility of such voting and shall share the results with the Government, which shall, within fifteen days from the commencement of a session of a House after the receipt of the report, lay the same before both Houses of Majlis-e-Shoora (Parliament).*
>
> *(2) In this section, 'Overseas Pakistani' means a citizen of Pakistan under the Pakistan Citizenship Act, 1951 (II of 1951) or holder of National Identity Card for Overseas Pakistanis under the National Database and Registration Authority Ordinance, 2000 (VIII of 2000) who is working or residing abroad permanently or temporarily for not less than six months."*
>
> *[Emphasis supplied]*

The rulemaking power in this regard is vested with the ECP as contemplated by Section 239 of the Act which is reproduced as under:-

> *"239. Power to make rules.—(1) The Commission may, by notification in the official Gazette and publication on the website of the Commission, make rules for carrying out the purposes of this Act.*
>
> *(2) The Commission shall make the Rules under sub-section (1) subject to prior publication and after hearing and deciding objections or suggestions filed within fifteen days of the publication."*
>
> *[Emphasis supplied]*

4. Overseas Pakistanis have been conferred with the right to vote as per the interpretation of Article 17 of the Constitution undertaken

ATTESTED

Court Associate
Supreme Court of Pakistan
Islamabad

by this Court in Ch. Nasir Iqbal's case *(supra)*. Thus where the right of Overseas Pakistanis to vote already exists as per the law and is duly recognized, it must necessarily be given due effect. For this reason, the word 'may' appearing in Section 94 of the Act is to be read as 'shall' and to this end, the only step which the ECP has to take is with regard to adoption of a suitable and effective mechanism and procedure by making appropriate rules under Section 239 of the Act. Accordingly, Section 94 of the Act makes it mandatory for ECP to conduct pilot projects enabling Overseas Pakistanis to vote in the upcoming bye-elections. It is worth mentioning that the phrase 'pilot projects' in terms of Section 94 *supra* does not mean that the votes cast by Overseas Pakistanis through i-voting in the bye-elections, would be treated as mock votes in mock elections, or that the votes cast under such pilot projects would be invalid, rather they are to serve as a sample and if successfully accomplished, or if some technical problems or issues come to fore after removing the same, that this exercise of enabling Overseas Pakistanis to vote may then be replicated on a larger scale, i.e. for future General Elections. Besides, there is a safety net contained in the proviso to Rule 84-C(2) of the proposed rules for overseas voting. This allows ECP to direct exclusion of overseas votes from the final count if it is of the opinion that the technical efficacy, secrecy and security of voting has not been maintained or has for any reason been compromised. This clearly suggests that overseas votes are to be included in the result of the bye-elections unless excluded by the ECP for valid reasons. The purpose of such 'pilot projects', as has been made clear by Section 94 *supra*, is to ascertain the technical efficacy, secrecy, security and financial feasibility of such voting after which the ECP is required to prepare a report and submit it to the Government which in turn shall lay it *(report)* before both

ATTESTED

Supreme Court of Pakistan
Islamabad

the Houses of Parliament within fifteen days from the commencement of a session of a House after the receipt of the report.

5. According to the notification dated 17.08.2018 issued by the ECP regarding the programme of the next bye-elections for 2018, it is declared that bye-elections for 37 constituencies *(both National and Provincial)* are to take place on 14.10.2018. To our mind, undoubtedly these and subsequent bye-elections (*if any*) are visualized, and fall within the meaning of, 'bye-elections' as contemplated by Section 94 of the Act for the pilot projects that ECP has to conduct in order to enable Overseas Pakistanis to exercise their right to vote. As already observed Overseas Pakistanis are clearly entitled to vote in the General Elections; they are therefore equally entitled to vote in bye-elections that are held to fill vacancies which have or will occur. The system so tried, tested and perfected can then be deployed in the next General Elections.

6. To the aforementioned end, Rules 84-A, 84-B and 84-C of the Election Rules have been framed. According to the Secretary ECP, they provide for a computerized mechanism, i.e. I-voting, to enable Overseas Pakistanis to exercise their right to vote. The proposed rules are reproduced below for ease of reference:-

> *"84-A. Registration procedure for voting by Overseas Pakistanis.–(1) Where the Commission decides in terms of sub-section (1) of section 94 to make arrangements for voting by Overseas Pakistanis living abroad, it shall hold such voting through internet (I-voting).*
>
> *(2) Only those Overseas Pakistani voters shall be eligible for voting who possess:*
> *(a) valid National Identity Card for Overseas Pakistanis (NICOP);*
> *(b) valid Machine Readable passport (MRP); and*
> *(c) valid E-mail address.*

ATTESTED

Court Associate
Supreme Court of Pakistan
Islamabad

*(3) The Overseas Pakistani voter, desirous to cast his vote through I-voting from abroad, during registration time-period as may be fixed by the Commission, shall access the Overseas Voting System through the internet and shall create an account using following credentials:*

*(a) Name;*

*(b) Email address;*

*(c) Generating password of his choice;*

*(d) Mobile Phone Number (optional); and*

*(e) Country of Stay.*

*(4) A confirmation email of account so created shall be forwarded by the system to the applicant at his given email address and by clicking on the link therein the voter shall be prompted to provide the number of his Machine Readable Passport with its tracking identity and NICOP number along with date of issuance thereof.*

*(5) Upon completion of proceedings under sub-rule (4), a verification process will be initiated wherein random questions regarding voter's identity information shall be asked by the System and upon correct reply, a message of "Successfully verified" shall be displayed by the system:*

*Provided that a confirmation email of account verification shall also be forwarded by the system to the applicant.*

*(6) In case the voter could not correctly reply first set of questions mentioned in sub-rule (5), the system will allow multiple attempts to correctly reply failing which that NICOP number shall be restricted for further attempts:*

*Provided that upon successful verification, a unique passcode shall be forwarded to the applicant by the system through email before the polling day:*

*Provided further that on receipt of list, from the Commission, in respect of Overseas Pakistani voters registered as such, the Returning Officer shall take necessary steps to make sure that no overseas voter so registered for overseas voting is allowed to cast his vote at the polling station in person.*

ATTESTED

Court Associate
Supreme Court of Pakistan
Islamabad

*84-B. Voting procedure for Overseas Pakistanis.– On polling day, the voter shall log in to the overseas voting system using his username and password and shall avail the voting option from the system for casting his vote in respect of his National Assembly, or, as the case may be, Provincial Assembly Constituency by entering unique passcode:*

*Provided that by going through designated list of candidates of selected constituency, the voter shall cast his vote by selecting his desired candidate:*

*Provided further that upon successful submission of vote, a "confirmation" message shall be displayed on the screen.*

*84-C. Preparation of results in respect of Overseas voting.–(1) After the polling hours are over, the Commission shall generate the Form-45 (Result of the Count) in respect of the constituency by using Reporting Portal of the Overseas Voting System and send the same to the Returning Officer concerned immediately through quickest means as are available for the purpose.*

*(2) On receipt of Form-45 (Result of the Count) from the Commission under sub-rule (1), the Returning Officer shall include the results contained therein in the consolidated results of the count as furnished by the presiding officer to be prepared by him under section 95 in such manner as the Commission may determine:*

*Provided that the Commission may direct for non-inclusion of the result in respect of the Overseas voting during consolidation of results under section 95, if in its opinion, the technical efficacy, secrecy and security of the voting has not been maintained during the said voting."*

The ECP and NADRA had given presentations to this Court in the foregoing regard and about third party validation that has also been received from independent experts, regarding the safety, integrity and workability of the system. Based on these representations we *prima facie* find the mechanism of I-voting to be safe, reliable and effective for being utilized in a pilot project. We are sanguine that the aforesaid proposed

ATTESTED

Court Associate
Supreme Court of Pakistan
Islamabad

rules shall be incorporated in the Election Rules, 2017 to enable Overseas Pakistanis to exercise their right to vote in the forthcoming bye-elections. However, we direct the results of the bye-elections and the vote count of the votes cast by the Overseas Pakistanis through the I-voting mechanism shall be kept separately and also secret till the time that ECP is satisfied about the technical efficacy, secrecy and security of the votes cast by Overseas Pakistanis through the I-voting system. In case such determination, made on the basis of reasons, is in the negative and the ECP is not satisfied about the integrity, safety and reliability of the systems and the votes cast through the same; ECP shall exclude the segregated votes cast by Overseas Pakistanis from the official result of the bye-elections in accordance with the proviso to Rule 84-C(2) *supra*. This safety feature shall ensure that the elections are founded upon verified and authenticated votes only.

7. Before parting we would like to express our appreciation for the dedicated efforts of NADRA and ECP undertaken for this noble purpose of great constitutional importance. The petitions are allowed in the aforementioned terms.

Sd/- Mian Saqib Nisar, CJ

Sd/- Umar Ata Bandial, J

Sd/- Ijaz ul Ahsan, J

Certified to be True Copy

Court Associate
Supreme Court of Pakistan
Islamabad

Lahore, the
17th of August, 2018
Not approved for reporting
M. Azhar Malik/*

28/8/18

19918/18
Date of Presentation: 28.08.18
No of Words: 3000
No of Folios: 30
Requisition Fee Rs: 60
Copy Fee in: 18.00
Court Fee Stamps: 23.60
Date of Completion of Copy: 28/8/18
Date of delivery of Copy: 28-8-18
Compared by:
Received by: