1. Executive Summary

1. The Westminster Foundation for Democracy (WFD), together with input from its partners, the Electoral Institute for Sustainable Democracy in Africa (EISA) and Democracy Reporting International (DRI), has conducted an independent and technical review of the voting machines procured by the Commission Électorale Nationale Indépendante (CENI) for use in presidential, legislative (National Assembly) and provincial elections which are scheduled to take place in the Democratic Republic of Congo (DRC) on 23 December 2018.

2. The report describes the capabilities of the machines and their main security features, identifying risks to be mitigated, and proposing potential improvements. Although the CENI is unique in using this type of machine for elections, the report refers to best practices in election governance and lessons from the introduction of electronic voting in other developing countries (e.g. India, Brazil). It concludes by summarising the key points of attention, i.e. recommendations to address the highest impact and most plausible risks.

3. This review is not a comprehensive audit of the voting machines. Nevertheless, first-hand experience of using demonstration models coupled with technical working sessions with IT experts from the CENI provides an opportunity for tentative analysis. Legal and constitutional provisions governing the introduction of voting machines and concerning results transmission procedures, as well as wider aspects of governance and the electoral systems and management are beyond the mandate of this review.
2. Overview of Technical Capacity

1. The CENI has worked with Miru Systems in South Korea to develop a voting machine which is capable of printing ballot papers for counting by hand and keeping an electronic tally of votes cast. The device resembles an Android smartphone or tablet equipped with an internal thermal printer and scanner, while it logs votes cast in a manner comparable to a direct-recording electronic (DRE) voting machine. DRE is one particular type of electronic voting machine that has been used to administer elections in Belgium, Brazil, India, Namibia, and Venezuela.

2. The device runs a proprietary software application developed by Miru Systems using the programming language Java, and compatible with the Android Operating System (OS). The OS is configured in kiosk mode, so that when the device is powered on, the voting application boots up automatically. This renders the Android OS inaccessible to voters.

3. Technicians can access the OS by rebooting the device and repeatedly tapping the screen in a particular location. This activates a credentials screen, where the technician must enter an administrator password. Once access to the OS has been granted, it is possible to view the application files, databases, and external and internal hardware devices. Currently, devices used for training have a default administrator password, but the CENI intends to create unique passwords for each technician on the final version of the machines. This should reduce the risk of an information security breach.

4. The first prototype model, known as P1, arrived in the DRC in August 2017. Trials were conducted, resulting in the development of the second prototype, P2, in January 2018. The final model, referred to as P3, was launched in February 2018. P3 integrates the following major changes:

   - Introduction of a removable internal battery pack, enabling expired or faulty parts to be replaced without opening the machine (as shown in Figure 1 below);
   - Increase of the voltage of the battery from 12 volts to 24 volts;
   - Replacement of the internal printer feeding plate with a more durable metallic one to avoid warping during prolonged periods of use;
   - The incorporation of a WiFi interface;
   - Enabling the scanner to read and process the *Procès-Verbal* (PV) results sheet (although it remains unclear whether this function will be used for elections taking place in 2018);
   - An additional 1 GB of memory in the device; and
   - An increase in software security from AES 128-bit encryption to AES 256-bit encryption, including the SQLite database.
5. The CENI has followed a rather unique testing cycle, developing the three prototypes through simultaneous training and testing, and then re-testing adjustments made. This approach does not reflect best practice, which generally divides the process into three phases: requirements gathering, development, and testing (incorporating functional, non-functional, and full testing cycles). The implication of CENI following this unique testing cycle is that some important layers of verification are missing.

6. The original P1 model was shipped as standard with the Android OS Lollipop 5.0.2 API 21; while the P3 is shipped with Android Lollipop 5.1 API 22. This operating system was first released in late 2014 and was superseded in 2016. As such, security patches for this version of Android are no longer supported. The CENI has not ruled out the possibility of updating the Android OS prior to the elections; however, the priority should now remain stability and usability. Significant testing would be required prior to proceeding with any update, lest it affect the interaction of components. The CENI could readily mitigate some of the potential security vulnerabilities by addressing points 5(c) and 5(d). Last-minute software updates could render the device vulnerable to possible security breaches, such as malicious applications bypassing the operating system’s protection systems, or the possibility of remote access by malintended users.

3. Security Features

1. The voting machine’s hardware and software security features are in line with those designed and developed by suppliers of similar devices; however, they could not be thoroughly tested by the assessment team. Human resource constraints at the CENI prevented the team from conducting a detailed examination of the software, source code, and database. Nonetheless, a brief description of the manner in which the machine is operated provides insight into each of the features.

Software and Data Security Features

2. The device’s software stack (OS, voting application and database) resides on the external SD card. Without the SD card the device is rendered “useless” – it is referred to as a ‘dumb terminal’. Upon insertion of the SD card the device becomes system operable and must then be deemed as sensitive.

3. The SD card includes a SQLCipher database (version 3.x.x). This is a specialised build of SQLite, a popular database system which uses structured query language to manipulate tables.
provides enhanced security, allowing for transparent and on-the-fly AES 256-bit encryption of the database file. The SQLCipher database is thus encrypted at file level, preventing access without the right credentials; however, the information stored in the database is a flat file (i.e. unencrypted text). The machine interacts with SQLCipher using a Java Database Connectivity API (a JDBC driver).

4. During the initialisation process, the software loads the relevant candidate and polling station data from the USB drive to the SQLCipher database on the SD card. The USB stick then functions as a permanent and continually synchronised back-up of data saved on the SD card.

5. Once in election mode, the machine conducts an integrity check on external drives. This renders it impossible to replace the USB stick containing candidate and polling station data with another one. In the event a machine breaks down, the USB stick and SD card could both be removed and replaced in another machine, provided they were in the same state. To read these external drives, the replacement machine would need to be “clean”, i.e. it had never been initialised. In this eventuality, the machine would resume the previous state, i.e. it would continue the election where it was left off.

6. Currently all log files (user logs and system logs) are saved on the SQLCipher database but are not accessible. To enhance maintenance, trouble-shooting, and provide scope for an audit, the CENI should make logs accessible to technicians; as proposed in point 6(b).

7. The CENI plans to prepare SD cards and USB sticks at its headquarters in Kinshasa and distribute these in Tamper Evident Envelopes (TEEs) to the regional training centres prior to the initialisation of the devices. Upon the close of poll on election day, the CENI intends for the SD card and USB stick to remain with the device and be transported together with the other sensitive material to the Local Results Compilation Centre (CLCR) in each region.

8. Currently each USB carries data for the entire country. The CENI has confirmed its willingness to produce one USB stick for each of the 26 provinces, as per point 6(f). This will both reduce the time required to prepare external drives and would greatly prevent errors from taking place (i.e. an operator in one part of the country misusing the machine to count for another constituency) as well as reduce the possibility of fraud. Additionally, it would reduce the amount of time required to copy data to the USB sticks.

9. Ahead of the elections, external storage devices (the SD card and USB stick) will need to be secured through software encryption tools to reduce the risk of malicious intent. While the CENI was aware of the importance of this step, it was not evident on the USB sticks used by demonstration models.

Set-up processes

10. Prior to election day, the device must be initialised. The necessary steps should be documented in the Polling Station Process and Procedures Manual, which is currently in draft form. On the current models, used for training, a technician inserts an initialisation card, containing a security QR code. The machine displays a set-up screen including a number of parameters. The technician selects a location and confirms which election data should be loaded.

11. On election day, the polling station president – together with the polling staff, political party agents and observers – ‘open’ the voting machine. The technician inserts a poll opening card, which provides an opportunity to review the settings, and to amend or confirm the polling station address. After this point no further changes are possible. The CENI plans to have polling station staff sign the poll opening card; however, the process could be further improved if political party agents and observers witnessing the process were also invited to sign the card, as outlined in point 7(d).

12. In future elections, the CENI might decide to alter these configuration processes by printing initialisation and poll opening cards with QR codes which have the relevant configuration settings
embedded in them. Including additional data in the QR codes would prompt the machine to load locality and election settings from the USB stick, obviating the need for a technician to manually select these settings. Verification safeguards could be incorporated, such as requiring the polling station president to approve the settings by typing in a unique password or PIN code.

13. At present, the machines used for training purposes contain a function to print QR codes on blank ballot cards. Ahead of the elections, ballot cards will be manufactured in South Korea, and contain a QR code unique to each constituency (electoral district). These pre-printed polling cards will be shipped in the carry case alongside the machines. Polling cards for one constituency will not be accepted by machines configured for another. This feature is designed to prevent electoral fraud; however, it is contingent on the CENI ensuring that the number of ballot cards issued per machine reflects the number of registered voters at each polling station, as outlined in point 7(a).

14. The CENI’s preferred method of tackling ‘over-voting’ focuses on the reconciliation process, rather than limiting the number of ballot cards per machine. The CENI intends to reconfigure the machine so that it records (a) the total number of paper ballots received; (b) the number of valid votes cast; (c) the number of invalid votes cast; (d) the number of spoilt ballots (*bulletins nuls*); and (e) the number of unused ballots. These figures should tally.

15. During the voting process, the ballot card is inserted into the device, the QR code is checked, and if valid, the system allows voting to proceed. Once the voter has selected their preferred candidates for the presidential, National Assembly and provincial elections, the machine prints those choices on three separate sections of the card, using the internal thermal printer. The card is then ejected from the device, the vote is recorded in the database, and the voter inserts the ballot in the ballot box.

16. If the machine were to fail prior to printing (due to a power cut or printer malfunction), it would still be possible to complete the vote upon re-booting. This is because the vote is not recorded until after printing. Each polling card can only be used once.

17. Currently, the machines will read a ballot card even if it is inserted incorrectly, i.e. with the arrow facing in the wrong direction. As such, it is possible to cast ballots for the presidential, National Assembly and provincial elections, with the first and last of these printed on the wrong section of the ballot paper. This would render the presidential and provincial votes on this mishandled ballot void at the manual count, while allowing the National Assembly vote to count. It would also create inconsistencies between the electronic and manual counts.

18. Although polling station staff will be on hand to assist voters, and to ensure that they correctly insert the polling card, there remains a risk of disenfranchisement. Should sufficient time be available to make the necessary changes, the CENI might consider reconfiguring the paper sensor – or altering the QR codes printed on ballot cards – so that the machine can only read ballots with the arrow facing in the correct direction. Alternatively, if time is short, the CENI could dispense with colour-coded sections of the ballot card, thus eliminating the issue entirely.

**Hardware Security Features**

19. The machine is equipped with some major hardware security features:

- External communication ports are secured using a sealable and lockable flap; however, this does not fully cover one USB port, as outlined in point 5(a). It also raises key management issues, as explored in point 6(d);
- An additional security cover flap positioned at the top of the printer prevents the ballot card from being removed during the printing process (as shown in Figure 2 below).
4. Hardware

Physical Design

Figure 2: Front view of the device, showing the security cover flap on top of the ballot printer

Figure 3: Dimensions
1. The device is equipped with a 21-inch touch screen. It is shipped in an IP 65 carry case; however, the device itself does not carry that rating. This IP rating would indicate that the case is “dust tight” and not susceptible to water projected from a nozzle. The technical team did not have the opportunity to immerse the suitcase in water but pouring water over the case provided evidence that the seal was relatively robust.

2. The machine carries an internal battery pack purportedly capable of lasting for roughly six (6) hours, when fully charged. A secondary external battery pack is purported to last for twenty-four (24) hours, when fully charged, providing back-up. Neither the internal nor external batteries have been tested by the team, making it impossible to certify these figures provided by the CENI.

3. By law, polling stations must be open for eleven (11) hours, between 06:00 and 17:00. The CENI estimates that each voter should take around one minute or 60 seconds to vote. The fastest time that the technical team was able to complete the process was around 50 seconds, therefore it is likely that many voters unfamiliar with touch-screen technology will take well over one minute to complete the process. While it might be possible to attain the CENI’s estimates of 60 voters per hour, and therefore process the maximum number of voters per polling station (600) within the 11-hour voting window, this leaves no buffer for technological malfunction. The CENI should make a commitment to process any voters standing in line at 17:00, to prevent disenfranchisement.

4. Investments in voter education would likely contribute to reducing the average time taken to cast ballots. The CENI has already held electoral/education campaigns around the country, sensitising voters in urban centres to the machines. As outlined in point 11(d), a different approach will be required in rural areas, where familiarity with touch-screen technology is likely to be even lower.

5. Once the election campaign period begins, candidates and political parties competing in the election will have an incentive to educate their core voter base on how to use the machines. As with
the cumbersome paper ballot papers used in the past, parties will aim to raise awareness of the number(s) allocated to their candidate(s). The machine has the capacity for voters to type in the number associated with their candidate of choice. This has the potential to simplify matters, provided that the electorate is sufficiently well informed. The prospect of queues outside polling stations could offer a final opportunity for voter education, targeted at those waiting in line.

5. Potential Hardware Improvements

The following technical adjustments could be made to the hardware, provided these refinements do not result in a delay to the electoral process:

a) **Cover all external ports:** Figure 5 above provides a side view of the machine, displaying the connection (ethernet) and external drive (USB stick, SD card) ports. A security flap covers the connection and external drive ports to prevent access to the ports once closed; however, one USB port is not covered by the security flap. All the connection and external drive ports should be sealed to prevent unwanted access to the ports during operations on election day. If it is too late to redesign the security flap, the exposed USB port should be plugged and covered with a security seal.

b) **Review processes around the SIM card:** The CENI explained that a SIM card will be inserted into the device at the point at which the presiding officer and the technician configure the device, one or two weeks ahead of election day. The CENI should review its approach and consider inserting the SIM card only when data is to be transmitted to the central server. This would prevent a possible communication bridge (a link between the voting machine and an external device) being established, and thus rendering the machine vulnerable to unsolicited connections during operations on election day.

c) **Disable the WiFi by default:** In addition to the SIM card, the device is equipped with a WiFi antenna. As above, this allows for a potential communication bridge. Therefore, the WiFi antenna should be disabled at the point at which the technician transfers the machine to the presiding officer. This entire handover process should be documented and follow a step-by-step procedure which political party agents can observe and verify. If required at a later date, it should be re-enabled by a technician, and this process observed, verified and documented.

d) **Develop procedures for managing security flap keys:** The security flap which closes and prevents access to the communication, USB and external drive ports has been redesigned to allow for a padlock to be fitted. However, to manage 102,000 sets of individual keys poses its own separate problems. The CENI must ensure that all padlock keys – both the master and secondary duplicate – are kept in numbered key lockers which are tightly controlled and managed. Ahead of polling day, padlock keys could be transported with the device or in TEEs, much as the USB key and SD card will be.
6. Potential Software Improvements

The following technical adjustments could be made to the software, provided these refinements do not result in a delay to the electoral process:

a) **Limit the total number of ballots permitted on each machine**: There is currently no cap on the maximum number of ballots which can be cast on one machine on one day. As a result, each device can process as many votes as ballots are available with the correct QR code. A maximum of 600 voters are allocated to each polling station. The CENI has made allowances for a further 10% votes to be cast from supplementary lists, in line with international standards. It is recommended that the CENI introduce a maximum limit of 660 ballots per machine per day.

b) **Create a separate log file for audit purposes**: The CENI explained that all operations on the device are recorded in a log file saved in the database, complete with time-stamps. Records are made when turning the device on, initialising it, setting up the device for operations, and as ballots are cast (with the exact time recorded). The CENI should create a separate database log file for audit purposes.

c) **Restrict the available election categories to those conducted in December 2018**: The application has two election categories: indirect election and direct election. The presidential, National Assembly and provincial elections are selected through the direct election tab, while others can be activated through the indirect election tab. Indirect elections are not relevant to the current electoral cycle. The CENI should remove the indirect election tab to ensure that the technician does not accidentally or wilfully select and activate the wrong election type. In the same vein, four elections are currently loaded in the direct election tab: presidential, legislative (National Assembly), provincial and local government. Local government elections are not relevant to the current electoral cycle. The CENI should remove the local government option for the same reason outlined above.
d) **Remove QR code printing function:** The machine currently has a feature enabling it to print QR codes onto blank ballot cards. This has been used for training purposes. The final election software must be used only for polling and not have features which were designed for training purposes.

e) **Include essential polling station information on all cards used for opening and closing process:** After completing each major step (initialisation, poll opening and closing), data is printed on the respective cards. This currently includes polling station name, address, polling station number, and the names of the polling station staff. Each of the three cards should detail the total number of votes cast, i.e. on initialisation and opening the card must show a zero (0) value. In Brazil, when the polls open the voting machine prints a report called ‘zerisma’, that indicates no votes are pre-recorded on the machine. On closing it must reflect the total number of votes cast. This can be used as a transparent validation and verification step for observers and party agents.

f) **Restrict data on the USB to the province relevant to the device:** The candidate database contained on the USB currently includes all candidates for all election types for the entire country. The data should be limited to a province, i.e. creating 26 different databases containing the relevant data, multiplied by the number of machines being deployed in that particular province. This would greatly prevent errors from taking place as well as reduce the possibility of fraud. Additionally, it would reduce the amount of time required to copy data to the USB sticks.

g) **Revise candidate selection and confirmation process:** Currently, a voter selects their candidate of choice from those displayed. The application then brings up the selected candidate in a bigger window, with a larger picture of the candidate and two boxes below. One box is green, and the other box is red. The voter either selects the green box to confirm their vote or the red to dismiss the candidate and return to the selection screen. However, if a user touches the picture of the candidate, the machine registers a vote for that candidate. The CENI should alter this feature so that votes can only be cast by touching the green box. The colour-blind may find it difficult to distinguish between the red and green, increasing the importance of voter education.

7. **Set-up Procedures**

With the possible introduction of voting machines into the electoral cycle a number of new procedures will need to be adopted. These will need to be well-planned and executed. At the moment, the lack of clear guidance or regulations is notable, and it is recommended that the CENI invest time in developing procedural guidelines and disseminating these widely. Some points of attention:

a) **Develop and disseminate clear procedural guidelines:** For the sake of transparency and efficiency, the CENI should clarify the role of the voting machine in different stages of the electoral cycle, and outline protocols concerning the handling, configuration and administration of the devices.

b) **Devise plans for storage and security of the devices:** The procedures for storing and securing the devices have yet to be clarified. Such a plan should include storage and security measures at all stages of the deployment of devices including but not limited to: (1) receiving stock from South Korea; (2) transporting received goods to the CENI storage centres; (3) transportation of devices to relevant distribution points; (4) storage of devices at distribution points; (5) while devices are in custody of polling staff; (6) on election day, and (7) when devices are returned after election day. Points 11 (b) and (c) outline some best practices from the introduction of new electoral technology in the developing world.

c) **Reconsider the time available for distribution of devices, potentially distributing devices through CENI Antennae centres, followed by training centres:** The CENI indicated plans
to distribute machines to polling staff at the end of the training. Some devices may be handed out to the polling staff up to two weeks in advance of the election day, while others will be distributed three days before the election day. Allowing several days is understandable given the necessary travel; however, leaving devices in the possession of staff for relatively long periods increases the risk of tampering. Where possible, this situation may be addressed by distributing the devices through CENI’s Antennae Centres, which serve the polling stations located nearby, rather than counting on staff to keep the machines secure for extended periods.

d) **Invite party agents and observers to CENI distribution centres**: The handover of the machine and its equipment should be witnessed by political party agents and observers. This would enable them to verify the steps taken by the technician configuring the machines. These should be limited to inserting only the USB memory card and SD card; locking and sealing the security flap; powering on the device and confirming the battery levels; configuring the machine to the correct polling station; verifying that the database presents a zero-value vote count; validating each of the candidates contesting the three different elections; and printing out the validation configuration report in front of the party agents and observers. If these steps are completed correctly, the party agents and observers should sign the handover form, which records the serial number of the plastic seal used to close the carry case as well as the total number of ballots allocated to the polling station. Party agents and observers should be informed about the functioning of the machines and trained in observing their configuration and use in order to know what to pay attention to whilst observing elections and make an effective observation possible.

c) **Ask party agents and observers to sign validation cards**: As the presiding officer initiates the machine for voting at the polling station, party agents and observers should again be invited to monitor the process. This would enable them to verify that the machine is configured for the correct elections (presidential, National Assembly and provincial); and that the device displays all of the candidates for that constituency. If satisfied, the party agents and observers in attendance could sign the validation cards.

8. **Technical Support**

1. The CENI intends to establish approximately 21,000 polling centres and some 75,568 polling stations. Each polling centre will be responsible for providing support to a maximum of five polling stations. A technician will be on standby to assist with basic technical support and potentially deploy a replacement machine, in the event that one of the polling stations requires a new unit. Additionally, 232 national training centres are to be equipped with a senior technical staff member (trained by Miru Systems) with access to replacement hardware (batteries, printers etc.) ahead of polling day. The CENI’s headquarters in Kinshasa will log high priority technical issues and endeavour to resolve these as quickly as possible.

2. Planning could be improved by preparing comprehensive procedures for different eventualities. As outlined in point 5(f), the CENI should develop detailed support plans for different hypothetical technological failings; for example, the malfunction of devices and external drives (USB sticks and SD cards). These plans should outline step-by-step procedures for the replacement of voting machines and external drives so that they can be immediately put into action if required.

9. **Results Tabulation**

1. The results tabulation process is outside of the mandate of this review, yet it is a vitally important process within the electoral cycle, and one where the role of the voting machines requires greater clarity. This report examines only the technical capacity of the voting machine, not any legal or constitutional provisions regulating its use.
2. The Congolese machine is unique in printing paper ballots, maintaining an electronic tally, and being equipped with the means to transmit results. The lack of comparable devices means that there is little scope for drawing on best practice or lessons from other contexts. In the absence of clear guidelines or recommendations from other contexts, there is a risk that the CENI struggles to manage multiple and potentially contradictory sets of electoral data, leading to confusion during results tabulation.

3. Congolese electoral law provides for the *Procès-Verbal* (PV) results sheets to be the only definitive reporting mechanism. According to the CENI, the original manual count PV results sheets will be sealed in TEEs and transported to the Local Results Compilation Centres (CLCR) for processing.

4. The machines have the technical capacity to scan, read and transmit the data on the PV results sheets. This feature is not intended for the elections scheduled to be held on 23 December 2018. In late July, the CENI outlined plans to transport voting machines to CLCRs, where PV results sheets are collated regionally to calculate the outcome of the three elections. Under these plans, it would be at the CLCR level that machines would transmit data to the national level. If the CENI intends to follow this procedure, rather than transmit data from polling stations as initially outlined, then it is all the more important to remove the SIM card and disable the WiFi antenna, as outlined in points 5(b) and (c).

5. It is understood that electronic voting figures, calculated by the machine based on votes cast, will be used only for validation purposes, and to dissuade electoral malpractice. In the case of discrepancies between the manual and electronic returns, the manual results will prevail. The CENI should ensure that the purpose and hierarchy of the different results is made clear in the Polling Station Processes and Procedures manual, which is currently being finalised.

6. In light of the uncertainties and risks outlined above, the CENI should clarify the role of the machine in the transmission of results, particularly concerning the weight given to, and the use of, electronic results generated by the machine, *vis-à-vis* the manual return.

**Results transmission capacity**

7. At the technical level, the machines have four means of external connection:
   - GSM – using an internal SIM card (where network coverage permits);
   - Satellite – using a satellite router (for areas that are not covered by GSM networks);
   - Local Area Network (LAN) – using the Ethernet port;
   - WiFi – using the in-built antenna.

These are purely technical observations, and not a reflection of the legal or constitutional provisions governing election results calculation or transmission.

8. If using GSM or satellite connections, each device will be assigned a unique IP address, which will only allow for transmission; devices will not be able to receive data (a good network security parameter). Both networks should allow for security protocols to be configured, such as VPN/APN tunnelling, with the result that data over the network can be scrambled and encrypted (AES 256-bit).

9. The CENI currently has 157 sites covered by the satellite network and planned to expand this to 232 by the end of July 2018. If using the LAN port or WiFi antenna at the CLCR level, the machines will be able to connect to a server. Each CLCR will be served by a satellite connection using the Very Small Aperture Terminal (VSAT) model, which does not require line-of-sight.
10. Once the networks have been brought online, the CENI should conduct a simulated test to ensure network connectivity to main hubs. Additionally, a security audit should be carried out to verify the networks and ensure no unwanted connections are able to access the system.

Data management

11. Given the existence of two sets of data (manual and electronic results), the CENI should clarify precisely what protocols exist for handling potentially contradictory results, and how this data will be managed at regional and national levels – as well as the degree to which party agents and observers will be privy to these processes.

12. Clarification from the CENI as to the protocols and safeguards it has put in place will reassure electoral stakeholders; therefore, it is recommended that the electoral commission prepare a set of guidelines codifying the role of the machines in results transmission and the protocols in place.

13. Data management guidelines should also outline the operational procedures to be followed during the preparation of the database, system initialisation, and data transfer from the machines after polling. Guidelines should also outline the necessary steps in recovering data from a machine that malfunctions during the election and transferring the USB stick and SD card to a “clean” machine, as outlined under section 3.

Regional tabulation centres

14. The CENI has plans to establish 171 regional tabulation centres, mirroring the number of candidate processing centres (BRTC). Drawing on international best practice, the CENI should:

   a) Introduce incremental reporting at predefined times so as to avoid long time delays between results reporting;
   b) Establish a mechanism to verify any results transmitted electronically via the devices, whereby the server acknowledges the total results received from each machine;
   c) Follow sterile environment deployment guidelines at the tabulation centres, with individuals tallying separately (i.e. data entry 1 and data entry 2 unable to communicate). This is known as a double-blind entry and is an internationally recognised standard;
   d) Ensure that result tallies from manual counts and electronic machines are made available for cross validation.

15. The CENI plans to allow observers, party agents and the media at the tabulation centres; however, individuals need to be trained on what to look out for and how the process takes place. Training will need to be provided to various stakeholders to ensure they understood how the process works and what issues to consider.

10. Institutional Capacity

1. A number of the issues raised above hinge on the capacity of the CENI to manage processes, both technically and logistically, which in turn is dependent on systems in place and human resources. In order to deploy new technology for election purposes, CENI staff need to be well-trained and must understand the machine. This will ensure both its successful deployment and operation during the election, as well as visibly demonstrating to the electorate that the CENI is prepared and honouring its mandate.

2. The task of ensuring sufficient and well-trained technical staff would be a challenge for any electoral commission, no matter the context. The process of preparing for any elections in a country is
a considerable task; and with the introduction of new technology it has become even greater, requiring further capacity and even more defined processes and procedures, alongside consultations, communication and information.

3. The recruitment and training of polling station staff and technicians should be a priority area of attention. CENI staff will require not just education but basic IT skills and familiarity with the machines if they are to properly operate the machines and guarantee the integrity of the elections. The electoral commission intends to train trainers at the national level and then cascade trainings to the provincial levels.

4. According to the legal framework, each polling station requires five polling staff, and the CENI plans to train all five staff in the use the machines. The electoral commission will also train one additional back-up staff member per polling station, who will be brought in if a core member fails to attend. It remains unclear whether these back-up staff will be able to stand in for a senior official, such as the presiding officer or secretary, or whether others would need to be promoted to carry out those roles. No one should perform key election duties if they have not received the necessary training.

5. The CENI must ensure that sufficient machines are available for training purposes and ascertain that staff have ample opportunity to use them through organising dry runs. In the Philippines, for example, a post-election review found that not all regional training centres were equipped with electronic voting machines, thus depriving electoral commission staff of the opportunity to familiarise themselves with the technology. Lessons from India suggest that devices used for training purposes be kept separate from the machines to be used for polling.

11. Lessons from Other Countries

   a) Building trust in new technology in India, Namibia, Brazil and the Philippines

1. The need for an electoral commission to build confidence in the introduction of new technology through incremental change is illustrated by the case of India, where the introduction of electronic voting machines (EVMs) started in 1982 with a limited number of machines being tested during a by-election in Kerala. The Election Commission of India updated the legal framework used to regulate the elections, clarifying the role of the voting machines in different stages of the process, and promoting predictability and stability. The Indian EVM enjoys a high level of public trust, and while the machine has been challenged in the courts, electoral fraud has never been proven.

2. Namibia began debating the use of EVMs in 2004, and amended the electoral laws in 2009, before finally testing the machines in a series of by-elections during the course of 2014 ahead of their use for presidential and legislative elections that November. Brazil commenced the introduction of electronic voting in 1996, but only proceeded to a full roll-out by 2002. Brazilian election governance and management structures took an approach that addressed not only their internal team’s readiness for the deployment of new technology but also considered the need to prepare the electorate at large about understanding and using the machines.

3. In a step designed to build confidence in the EVMs, the Brazilian electoral management body, the Superior Electoral Court (TSE) organises penetration testing of its machines by inviting teams of specialists from the police and security services and “ethical hackers” to identify potential vulnerabilities. IT experts are given access to the EVMs in a controlled environment to check hardware and software capabilities. Participants in the “hackathon” present their findings to the TSE, which it uses to review and refine its information security protocols. The process results in the
4. By contrast, the Electoral Commission of India (ECI) does not allow independent evaluation of the machines or source code. The ECI established its own technical evaluation committee responsible for assessing the machines by evaluating functions and design features. This provides less scope for computer security experts to test the machines, as the members of the committee must evaluate the machines based on information provided by the ECI alone.

5. In the Philippines, the Commission on Elections (Comelec) established multiple bodies to assess a new automated election system (AES). Comelec appointed an advisory council, comprising representatives from government, academia, the IT industry and civil society, which helped the electoral commission to evaluate the technology, identify potential issues, support the procurement of machines, and evaluate the AES. Additionally, Comelec appointed a technical evaluation committee, including representatives from government, industry and civil society to certify hardware and software components. The Filipino parliament also formed different committees: the House Committee on Suffrage and Electoral Reforms, and the Joint Congressional Oversight Committee on the AES. Finally, Comelec hired an independent US based firm, SysTest Lab, to evaluate software and hardware and recommend improvements.

6. Should the CENI wish to follow suit, it could start by organising further working-level sessions with IT experts from the political parties, civil society and academia, enabling them to carry out a preliminary assessment of the EVM. The certification and independent evaluation of the electoral technology is an ongoing process, and therefore it is never too late or too early to start.

7. Elections are a public exercise and hence maintaining transparency in the electoral process is essential and linked to trust in the poll. Regardless of election methods being used, election management bodies can build trust by promoting transparency in different aspects of the elections. In India, for example, the ECI invites party agents to observe the transfer of EVMs to returning officers and encourage them sign forms documenting their role. Returning officers also invite party agents to witness as they distribute materials to polling station staff. The ECI places responsibility on returning officers to ensure the presence of candidates or their agents and to provide them with a week’s notice of the processes to be followed. The ECI also allows party agents to follow vehicles which transport EVMs to different locations.

8. Both India and Bhutan organise pre-testing of machines before their distribution and in this regard send advance notices to parties. Likewise, Namibia and Bhutan allow party agents to take part in the distribution processes, but not to the same level as India.

9. The ECI devised protocols for the storage of machines covering the pre-election, election, and post-election periods. Protocols govern the access and locking of these storage facilities. Machines are generally stored in treasury strong rooms; but where such a facility is not available, the ECI hires a storage facility. The ECI maintains a log of who accesses the storage facilities and for what purpose. In case machines are repaired at storage locations, the details of repairs are entered into the log as well. The storage access protocols are also clearly defined with adequate security protocols. For example, two locks are placed on the doors of the storage facilities and the keys remain with two different individuals.

10. Civic and voter education in Brazil and the Philippines
10. Education is one of the most important aspects of any election, not only for polling staff but for observers and the electorate at large. When new technology or processes are introduced, educating the public on their use becomes critical to the success of the election.

11. An added value in many other contexts has been that involving civil society in voter education has resulted in such groups becoming strong advocates for the electoral process. The CENI should be aware of this opportunity to build citizen trust in, and support for, its work by involving non-governmental organisations in voter education.

12. In June, stakeholders articulated a concern that voter education on the use of the voting machines had been limited. This is problematic as in certain parts of the country people do not understand how touch-screen technology works. A lack of voter education could, conceivably, deprive people of their fundamental right to vote – or inadvertently result in them casting their vote for the wrong candidate.

13. The CENI should consider conducting voter and civic education exercises using different mediums (live demonstrations, brief videos capturing the process, television and radio plays, cartoons/bandes dessinés etc.) and in the different national languages (Lingala, Kikongo, Swahili and Tshiluba).

14. Ahead of the introduction of electronic voting in Brazil, the electoral management body hired a private firm to conduct a voter education drive. Mass media campaigns on television, radio and in newspapers were accompanied by local demonstrations, lectures, and even mock elections. More recently, the Philippines undertook a similar voter education drive. An independent survey of the electorate identified an increased level of awareness of voting procedures as result of the education drive.

12. International Standards of Best Practice

This report has highlighted a number of recommendations, some of which will be easier to address than others at this stage in the electoral cycle in the Democratic Republic of Congo.

The framework used for this assessment were international electoral standards and guidelines on good practices in implementing electoral technology and observing the use of technology in elections. The use of such a framework makes an assessment objective, independent and neutral as it is grounded in established standards and widely respected guidelines. The framework of these accepted standards and good practices can also allow election management bodies to ensure that the governance and management structures are at a level that will facilitate a successful deployment of new technologies in a seamless manner accepted by all stakeholders.

From this perspective, the guidelines on the introduction and observing electronic voting technologies suggest the following considerations as technologies are introduced in electoral processes:

- Define clear objectives for introducing voting technology as well as the problems that the technology intends to address;
- Develop the necessary legal framework to support the introduction of voting technologies to ensure the predictability and stability of the process;
- Carefully consider challenges in introducing voting technology, which is not perfect and brings the different types of problems voting machines generally have;
- Ensure trust and buy-in of all stakeholders in the technology being introduced;
• Ensure independent certification and auditing of the voting machines;
• Review internal capacity and staffing needs and hire additional staff as required;
• Develop the staff’s professional development plans and conduct voter and civic education exercises;
• Develop necessary safety and storage systems for the voting machine facilities;
• Consider the sustainability of devices including their upgrades, replacements and adjustments as per changing electoral conditions.

13. Summary of Key Points of Attention

Our first Voting Machine Review in DRC has been limited in scope as the team has not been able to carry out audit and certification of software and hardware or take account of many of the international standards listed above. Our assessment is therefore restricted to the machine’s functions as we operated it and the hardware and software features as explained to us by CENI. The list of our recommendations below is therefore not comprehensive, but rather intended to propose steps to mitigate the highest impact risks (both in terms of their potential effect on election results and popular trust in the process) and those with the greatest probability (both in terms of the likelihood of the risk, and the feasibility of it being addressed in the time remaining).

In conclusion to our Voting Machine Review we recommend that the CENI should at a minimum consider implementing the following steps ahead of the use of the machines:

- Disable external communications (SIM card and WiFi) until these are required;
- Cover all external ports (either alter the security flap or plug the exposed USB port);
- Set a maximum of 660 polling cards per machine per day to prevent over-voting;
- Remove the QR code printing function;
- Ensure that incorrectly inserted ballot cards do not result in invalid manual votes;
- Restrict data on the USB to the provincial level;
- Revise the candidate confirmation process to remove the function whereby touching the picture of a candidate registers a vote for them;
- Develop and disseminate clear procedural guidelines concerning the role of the voting machines, in addition to protocols concerning their handling, configuration and administration;
- Review distribution processes to minimise the amount of time the machines spend in the custody of polling station staff;
- Invite political party agents and observers to distribution centres;
- Involve political party agents and observers in pre-checks;
- Prepare detailed operational plans for replacement of hardware and external drives;
- Organise dry runs to enable polling station staff to gain experience of the machines;
- Prepare for queues and commit to process voters standing in line at the close of polls;
- Create a separate log file for audit purposes.

See the ACE Elections and Technology Guide, http://aceproject.org/ace-en/topics/et/eth/eth02/eth02b/eth02b3


Electoral Commission of India FAQs, http://eci.nic.in/eci_main1/evm.aspx


The international electoral standards are grounded in international human rights law. The International Covenant on Civil and Political Rights is the main source along with its authoritative interpretation in general comment 25 by the UN Human Rights Committee. For details see: Election Obligations and Standards, by the Carter Center, https://www.cartercenter.org/resources/pdfs/peace/democracy/cc-oes-handbook-10172014.pdf, accessed on 15 August 2018.