C.A.S.E.
Citizens' Alliance for Secure Elections

DEDICATED TO ENSURING SECURE, RELIABLE AND VOTER VERIFIABLE ELECTIONS IN OHIO

BEST PRACTICES

(Summary)

TO INSURE SECURE, RELIABLE AND HONEST ELECTIONS IN OHIO

The following document is a composite summary of the most significant "Best Practices" procedures recommended by the following organizations, with primary emphasis on the recommendations from the EAC. The separate details of each organization's recommendations can be found by selecting the appropriate link:

- Elections Assistance Commission (EAC)
- Cal Tech/MIT Voting Technology Project
- Brennan Center for Justice (NYU School of Law) and the Leadership Conference on Civil Rights
- NSF / Harvard Symposium on Voting
- National Ballot Integrity Project
- League of women Voters
- CASE Ohio

For ease of reference this document is divided into the several sections. Select the link to access the specific section desired:

I. Best Practices in Administration & Security for All Voting Systems

Voter Outreach

1. Sample ballot and, if practical voting machines, should be taken out into the community – shopping malls, churches, high schools, public meetings, etc. – to demonstrate how to properly complete it
2. A voter education program should be conducted to inform people who move, who change their name, who are released from jail after a felony conviction, etc. of need to reregister in order to be able to vote
3. A voter education program should be implemented using the media, video clips and public service announcements to educate voters about the voting process.
4. Include explicit instructions when sending out absentee ballots to inform the voter that the ballot will not be counted if it is not received in time, or if it is soiled or bent.
5. Pre-election Notices to the Voters as to when and where they should vote

Poll Workers

1. Implement a "Partners in Democracy" Program to Attract and Retain Younger Pollworkers: College Pollworker Program, High School Student Pollworker Program, Adopt-a-Poll.
2. Include training on Help American Vote Act (HAVA) requirements. For maximum retention by pollworkers, training should occur as close to Election Day a possible (but optimally not more than six weeks prior).
3. Consider multiple shifts for precinct workers. One might split the day into two eight hour shifts.
4. Consider shorter shifts to handle the peak hours, as is done with many service operations.
5. Evaluate pollworker performance via analysis and tracking of errors to a specific precinct. Use the analysis to constantly improve your training approach and materials…and to help select the best pollworker teams.

Election Operations/Security

1. Test every piece of voting equipment prior to deployment, using the ballot styles for that election. Invite the public and media to a "public test of the system."
2. Ensuring Transparency to bolster public confidence, take steps to make every component of administering your voting system as transparent as possible. Invite the public and media to view all aspects of testing.
3. Require staff and pollworkers to keep an Election Day "problem log" for all problems that are reported and how they were handled.
4. Establish a chain of custody to protect all ballots in the polling place (including provisional ballots, emergency ballots and absentee ballots dropped off at polls).
5. Security tape with sequential serial numbers must be used. A log should be maintained each time the seal is broken. The log should include the date, time, and person accessing the secured item, along with the serial number of the old security tape that was broken and the number of the next security tape that is placed on the secure item. If the serial number of the new security tape is not the nest sequential number then a breach of security has occurred.
6. If you are modeming in your unofficial results, use a phone line – not a wireless connection – and ensure the modem encrypts the information.
7. Voter-verified paper ballots for all federal and state offices (including printed ballots, optical scan/mark sense and punch card ballots, as well as voter verified paper ballots produced by touch-screen machines). Those jurisdictions whose equipment does not produce such ballots must use printed ballots for all state and federal offices.

8. Hand-counting of all votes (cast both in-person and absentee, with witness signature) for federal and state offices, conducted by the election judges at the precinct/polling place, with citizen oversight and assistance, immediately upon close of polls, with the results of this hand-count serving as the official tally.

9. Vote totals recorded immediately upon completion of the hand-count in triplicate on official report forms and signed by all election officials and observers present.

10. Immediate public and prominent posting at the polling place of one signed copy of the official hand-count. All ballots sealed in the ballot box, along with all tally sheets and one signed copy of the official report form. The sealed ballot box and remaining signed copy of the official report form are to be delivered directly to the controlling election officials.

11. Official election results will be compiled directly from the signed tally sheets/report forms from each polling place. No central servers or other tallying mechanism(s) manufactured, sold, leased or promoted by any manufacturer or vendor of any type of electronic voting equipment may be used to aggregate these results. Election authorities must retain all paper ballots, tally sheets and all signed copies of the official report form, in a secure location until the statute of limitation expires.

12. The paper ballots shall be the only instruments possessing legal vote status, and the hand-count will serve as the official basis for all 2004 state and federal election results at each level and phase of the process.

13. Require bipartisan or third-party monitoring of sensitive election procedures.

14. Require transparency in the operation and management of voting systems.

15. Make "random" spot checks truly random by using a transparent and public method for random selection.

16. Allow the press, and any citizen, to audit if they pay for it. If they discover that the election was miscounted, reimburse them. Find ways to do these audits inexpensively.

17. Allow each party to select a handful of precincts to hand-audit. Discretionary audits shine light into any precincts deemed suspicious.

18. Require audits for insufficient randomness (e.g., three candidates get 18,181 votes; voters arrived in alphabetical order).

19. Consider a 100 percent audit of the paper ballots.

II. Punch Card Voting Systems

Voter Interaction with Voting System/ Voter Education

1. **Discourage butterfly and caterpillar ballot layout.**
2. **In order to reduce errant punches, use a custom-punched mask containing holes only for positions utilized.**
3. **Train pollworkers to go through with a demo ballot in each vote recorder to make sure it is not possible to punch through any areas where there are no contests for that election.**
4. **Check the clarity of ballot layout with a usability consultant or by testing with focus groups of potential voters.**

Problems with "Chad" – How do you treat unreadable punch card ballots?

1. **Encourage voters to remove chad from their own ballot.**
2. **Protect ballot from tampering during counting and post-election procedures.**
3. **Consult state policies or, if there are no state policies, establish county policies for what constitutes a vote.**
4. **Confirm with your vendor that their perforation template is sufficient cutting depth and position accuracy.**
5. **Stylus – Use a non-blunt, positive chad remover "PCR" needlepoint tip. It is more expensive but more likely to push chad through**

Providing Second-Chance Review with Punch Card Systems

1. **Clear instructions and good ballot layout are critical in preventing voter errors.**
2. **Encourage the voters – not the pollworkers! – to clean the chad off their own ballots.**

Testing/System Integrity

1. **Proof to ensure vote recorder pages are pointing to the right candidate and in correct order.**
2. **Pre-election logic and accuracy testing--Develop test deck – without vendor assistance – using an incremental test pattern that tests all voting positions. Conduct a pre-test by running the test deck through the ballot counter multiple times to verify that the test deck has been correctly marked.**
3. **Store sealed memory card in locked office; secure it after Logic and Accuracy test.**

Pe-election Management and Security

1. **Buy new card stock for every election (or at least buy new card stock for November 2004). Gives cleaner punches, avoids swelling and bowing.**
2. **Have your ballot counters professionally serviced before every election.**
3. **Establish policies to prevent poll workers from mishandling the punch card ballots. The policies are designed to ensure that no one should have the opportunity to alter or change the ballot in a way that will compromise the integrity of the ballot.**

Maintaining punch card equipment

1. **Blow out the chad from the counters (*chad receptacles*) after every election.**
2. **Establish procedures for "chad-picking." The process should be transparent. Have bi-partisan teams do the picking. Example - Ohio Advisory 2001-04 sets policies regarding canvass board inspection for and removing chad, remaking ballots, etc. for the purpose of determining what constitutes a vote.**

Protecting the security of printed ballots

1. **Use a certified print vendor and get the exact specifications from the vendor for the printing.**
2. **Keep every generation of every proof.**
3. **Seal the tabulation machine with numbered seals when election definition is loaded and then record the numbers in logbook.**

Chain of Custody

1. **Keep all communications with your print vendor and your programmer.**
2. **Keep a log of everyone who lays out, proofs, transports, stores, etc.**
3. **Never let a vendor proof your ballots.**
4. **Require electronic transmission of ballot format to/from printer.**
5. **Make time to proof every ballot, every version, every correction.**
6. **Establish security procedures for printing and shipping of ballots.**
7. **Bring candidates, voters and community organizations in to review. Also, post to your website.**
8. **Have security procedures in case of a disaster.**

Election Day/Election Night Security

1. **Develop accounting and documentation procedures to make sure you get the cards back from polls.**
2. **Segregate "hanging chad" ballots for challenge board to make decision.**
3. **Install a security camera where your ballots are stored and where you are counting.**

Post-Election Management and Security/Equipment maintenance

1. **Clean the chad out of the vote recorders after every election, attempted votes may not register.**
2. **Establish procedures for "chad-picking" at central ballot counting site. The process should be transparent and uniform statewide. Have bi-partisan teams do the picking.**

III. Optical Scan Voting Systems

Voter Interaction with Voting System/Voter Education

1. **Provide clear voting instructions with explanatory graphics, on the ballot if possible.**
2. **Provide a secrecy sleeve to cover the ballot prior to scanning and print instructions on the ballot sleeve.**
3. **To help voters properly cast a write-in ballot, use a secrecy sleeve. Use the language: "write-in, if any" to avoid overvotes.**
4. **To improve ballot layout: when you design the ballot, be wary of where absentee voters may fold the ballot. On certain systems, a fold through an oval will reflect a vote, causing an over-vote if another mark was made.**
5. **Avoid splitting races across pages and across columns to prevent over-votes.**

Providing Second-Chance Voting with In-Precinct Scanners

1. **Allow voters the opportunity to have their ballots scanned for error before leaving the pooling location and dedicate a pollworker to assisting voters with the casting/feedback function for major elections.**
2. **Establish procedures for resolving "unvoted" (damaged, defective or blank ballots) ballots left by "fleeing voter."**
3. **Have written procedures to determine voter intent for the purpose of "remaking" or hand counting ballots. If "remaking" ballots, use labels or overmarks so that voter's original marks will not be lost.**

Testing System Integrity & Security

1. **Test the calibration of every scanner prior to the election.**
2. **Conduct printing tests and quality control tests.**
3. **Lots of test ballots of every ballot style, with as many permutations and combinations of potential ballots as possible.**
4. **If test ballots are prepared by the vendor, they must be supplemented with additional test ballots made up by the county and/or interested citizens.**
5. **Hand tally machine generated results.**
6. **Ballot programming should be done by the county, NOT the vendor**

Protecting the security of printed ballots

1. **Use a certified print vendor and get the exact specifications from the vendor for the printing.**
2. **Develop procedures to make sure the printer did not mix up stacks of printed ballots.**
3. **Keep all communications with your print vendor and your programmer.**
4. **Track anyone who lays out, proofs, transports, stores, etc.**
5. **Never let a vendor proof your ballots.**
6. **Establish security procedures for printing and shipping of ballots.**
7. **Bring candidates, voters and community organizations in to review. Also, post to your website.**

Election Day Management and Security

1. **Log all seal numbers. Don't open it until all board members are together. Have two officials present when count packets of ballots.**
2. **Develop a troubleshooting plan. Define the response time - know how long it will take to get a troubleshooter to the polling place. Have satellite locations from which to dispatch technical people and replacement supplies.**
3. **Verify that the electronic and optical scan machines used are the same as the systems that were certified.**
4. **Establish procedures for determining voter intent using uniform vote counting standards and for counting ballots that cannot be scanned. The process for counting ballots should be open and conducted under bipartisan scrutiny.**

Post-Election Management and Security

1. **NIST recommends against using a wireless transmission mode. There are no wireless ("Wi-Fi") or international security standards for wireless transmission of data.**
2. **Have two pollworkers transport results.**
3. **Establish procedures for when security measures are not followed such as when materials come back unsealed or unsigned.**
4. **Ballot Reconciliation Audit: Do a precounting of stacks of ballots or you could compare the voter body count to the ballot count run through the scanner. This is so you know the number going in to the machine to be read. This is especially important in processing absentee ballots.**
5. **Audit of the machines after the elections. Select 5% of all the precincts, randomly selected and well-distributed over districts, with all the votes on those 5% manually counted and compared with the results of the machine count. BIP parallel testing is better.**

IV. Direct Recording Equipment (DRE)

Voter Interaction with Voting System / Voter education

1. **Develop a web-accessible sample ballot that shows each screen, including the instruction and ending screen.**
2. **Track over-vote and "under-votes." Develop Election Day procedures to help determine the nature and cause of under-votes and blank votes to determine whether they are genuine under-votes or the result of voter confusion.**
3. **Ask minority language organizations to review ballot translations.**
4. **If you find a higher percentage of voter error in certain communities, work with pertinent community groups to educate voters in those communities.**

Pollworker Training and Polling Place Procedures

1. **Use USB's as machine power source; connect each machine to a USB. Daisy-chaining machines may become a single point of failure. Have a back-up plan and train pollworkers on how to troubleshoot and report alleged "power failure" problems.**
2. **Pollworker Accountability. Establish checklists to track pollworker performance on key steps of DRE voting processes.**

Pre-Election Day Management and Security

1. **Rely as little on the vendor as possible; look for outside IT expertise if it is not available in house. Have either election staff or independent consultants design and run tests.**
2. **Establish a deadline for patches or modifications to prevent unnecessary confusion.**
3. **Ensure all software, including patches, is certified.**
4. **Develop sound documentation of all election administration procedures that will allow you to identify the cause of problems after an election. Keep a log of receipt of equipment and software, who performed the programming and testing, and delivery to staging area or polling place. all paperwork that may be relevant in recreating how a failure might have occurred.**
5. **Develop rules for access to any sensitive equipment.**
6. **Keep a maintenance log for all voting system equipment. This log should track who has had access to the machine(s).**
7. **Machine delivery: Conduct risk analysis of the delivery system, Develop checklist for delivery, Use bar-coding to ensure proper delivery of all machines to polling places.**
8. **Elections officials should hire a well-qualified, independent security team to examine the potential for operational failures of and malicious attacks against the jurisdiction's DRE voting system.**
9. **Elections officials should provide a thorough training program for all elections officials and workers on security procedures to ensure that security procedures, including those recommended by the independent expert security team, are followed even in the face of Election-Day exigencies.**
10. **Use of "tamper tape" (along with an access log) on vulnerable hardware components to ensure that attempts to breach those components are detectable, replacement of certain hardware components with less vulnerability, and new security procedures to compensate for an identified hardware design flaw.**
11. **All recording software should be openly audited in the same mode that is used to conduct the counts.**

12. **Elections officials should develop procedures for *random parallel testing* of the voting systems in use to detect malicious code or bugs in the software.**
13. **Voting machine software can be prepared to recognize when it is being tested, the most effective tests of a voting machine will be tests that are as nearly indistinguishable from normal polling place operation as is possible. The best proposal for this involves selecting the machines to be tested at the last moment, and testing these machines from the minute the polls open to the minute the polls close.**
14. **Elections officials should have in place a permanent independent technology panel, including both experts in voting systems and computer security and citizens representing the diverse constituencies involved in election oversight, to serve as a public monitor over the entire process outlined above and to perform a post election security and performance assessment.**

Election Day / Election Night Management and Security

1. **Provide a back-up plan in the event of machine failure.**
2. **Control access to the voter "smart cards."**
3. **Configure the polling place to allow full view by poll workers of voting and voter activity to guard against unauthorized access while protecting voter privacy.**
4. **Security tape with sequential serial numbers must be used. A log should be maintained each time the seal is broken. The log should include the date, time, and person accessing the secured item, along with the serial number of the old security tape that was broken and the number of the next security tape that is placed on the secure item. If the serial number of the new security tape is not the nest sequential number then a breach of security has occurred.**
5. **Develop a plan to provide Election Day technical support for pollworkers, including a troubleshooting checklist, a call center, and rovers.**
6. **Establish written procedures for handling Election Day equipment failure.**
7. **Ensure transparency in all aspects of the tabulation process, especially in the transport or transmission of results to the central election office.**
8. **Develop chain of custody for memory cards and machines.**
9. **Maintain and operate voting systems in isolation from networks and the Internet.**

Post-Election Management and Security

1. **Conduct post-election logic and accuracy testing of machines.**
2. **Conduct a post-election audit to reconcile all records, especially the number of voters and the number of votes cast.**