STATE OF COLORADO SECURITY PROCEDURES
For
Electronic Voting Systems

INSTRUCTIONS

Pursuant to Denver District Court order, the following security and contingency requirements are required by the Secretary of State for the November 2006 General Election. Following the election, permanent security and contingency requirements will be adopted as an Election Rule through the rulemaking process in accordance with article 4 of title 24, C.R.S., including public comment and hearing.

Each county is required to submit an updated security plan and additional documentation as noted below to confirm compliance. Security information shall be provided no later than October 20, 2006.

MINIMUM PHYSICAL SECURITY REQUIREMENTS

The following items represent the minimum security requirements for counties using electronic voting systems, which include the hardware, software, DRE components, optical scan units, and any accessory items used in the operation of the voting system.

General Requirements, Clarifications on Statements, and Definitions

a. At all times, removable cards and cartridges that store firmware, software or data are to be handled in a secure manner similar to the handling of paper ballots. This same basic principle shall apply to all V-VPAT records. When not sealed in voting machines, such cards and cartridges shall be transferred in secure containers with at least two tamper-evident seals with printed serial numbers, and the integrity and serial number of each seal shall be verified by election officials at shipping and receiving locations.

b. All documentation of seals, chain of custody, and other documents related to the transfer of equipment between parties shall be maintained on file by the Clerk and Recorder and is subject to inspection by the Secretary of State.

c. The chain of custody for each voting device must be maintained and documented throughout ownership or leasing of the device by the Clerk and Recorder.

d. Only deputized clerks or judges sworn under oath are allowed to handle ballots, which include V-VPAT records.

e. No additional or modified software developed by the Vendor that is not specifically listed on the Secretary of State's certificate shall be installed on any component of the voting system. Nothing in this provision shall preclude the use of commercial off-the-shelf (COTS) software.

f. As used in this document, to "date" means to note the month, calendar day, year, hour, minute, and whether the time is a.m. or p.m.

1. Physical Locking Mechanisms and Seals

a. DREs – all Direct Record Electronic Voting devices shall have tamper-evident seals with printed, unique serial numbers affixed as follows:

i. A seal is to be placed over any removable card or cartridge that is inserted into the unit, or over the door covering the card.

ii. A seal is to be placed over any card or cartridge slot when no card or cartridge is inserted into the unit.

iii. Tamper-evident, numbered seals shall be affixed across the seam at which the two halves of the exterior case of the voting unit join, with at least one seal for each of the four sides of the device.

iv. If the voting device contains one or more slots for a flash memory card, a seal shall be affixed over each flash card or each flash card slot, door, or access panel.

v. These same procedures also apply to the Judge's Booth Controller (JBC) unit for the Hart InterCivic System 6.0.

vi. All seals are to be verified by two elections officials.

b. V-VPATs – all V-VPAT units shall be sealed upon verification of no votes being cast on the paper record prior to being attached to a specific voting device. Seals must be verified by at least two election officials prior to the start of voting, and at the close of voting. V-VPAT records shall either remain in the V-VPAT canister, or be sealed and secured in a suitable device for protecting privacy or as described in Election Rule 11.

c. Remote or Central-count Optical Scanners – Optical scanners used in a remote or central tabulating location shall have tamper-evident seals as follows:

i. A seal is to be placed over each card or cartridge inserted into the unit, or over any door containing the card or cartridge.

ii. A seal is to be placed over each empty card or cartridge slot.

iii. All seals are to be verified by two elections officials.

d. Memory Cards/Cartridges – Each removable card or cartridge shall have a permanent serial number assigned and securely affixed to it.

The Clerk and recorder shall maintain a written log that records which card or cartridge and which seal number is assigned to each voting unit. Any breach of control over a card/cartridge or door or slot for a card/cartridge before an election shall require that the County Clerk be notified and follow the procedures specific to the incident as described in Section 10 of these security requirements.

2. Individuals With Access to Keys, Door Codes, and Vault Combinations

Counties are required to state the names and dates of CBI background check for employees with access to the following areas. Counties may request from the Secretary of State variance with the following requirements only in extreme circumstances.

For all counties, use of door codes, vault combinations, computer and server passwords, encryption key codes, and administrator passwords on voting devices shall be changed at least once per calendar year prior to the first election of the year. Only county employees may be given access to such codes, combinations, passwords, and encryption keys, pursuant to the following limitations.

The requirements for a county employee to be given access to a code, combination, password, or encryption key are as follows:

a. Counties over 50,000 registered voters:

i. A maximum of 6 employees shall have access to all areas of election-related work and storage.

ii. A maximum of 4 employees shall have access to the storage area for voting equipment.

iii. A maximum of 4 employees shall have access to the counting room or tabulation workstations.

iv. Each individual who has access to the central election management system or central tabulator shall have their own unique username and password. No individual shall use any other individual's username or password. Shared accounts shall be prohibited.

v. A maximum of 2 employees shall have access to the absentee ballot storage and counting areas.

vi. The county shall maintain a log of each person who enters the ballot storage room, including the person's name, signature, and date and time of entry.

b. Counties under 50,000 registered voters:

i. A maximum of 3 employees shall have access to all areas of election-related work and storage.

ii. A maximum of 2 employees shall have access to the storage area for voting equipment.

iii. A maximum of 2 employees shall have access to the counting room or tabulation workstations.

iv. Each individual who has access to the central election management system or central tabulator shall have their own unique username and password. No individual shall use any other individual's username or password. Shared accounts shall be prohibited.

v. A maximum of 1 employee shall have access to the absentee ballot storage and counting areas.

vi. The county shall maintain a log of each person who enters the ballot storage room, including the person's name, signature, and date and time of entry.

No other persons may be present in any of the listed locations unless accompanied by one or more employees with authorized access.

3. Temperature-controlled Storage

Counties are required to verify the temperature-control settings used with the following components of a voting system. Information submitted to the Secretary of State shall indicate the specifics for each type of component, as well as the specific environment used, which may include, but is not limited to controlled offices, controlled vaults, and controlled warehouses. The settings for temperature control must be at least the following:

a. Servers and Workstations – Servers and workstations shall be maintained in a temperature-controlled environment. Maximum temperature shall at no time exceed 90 degrees.

b. DREs – DREs shall be maintained in a temperature-controlled environment. The temperature settings shall be maintained at a minimum of 60 degrees and a maximum of 90 degrees.

c. Optical Scanners – Scanners shall be maintained in a temperature-controlled environment. The temperature settings shall be maintained at a minimum of 50 degrees and a maximum of 90 degrees.

d. V-VPAT Records – In addition to the requirements set forth in SOS Rule 11, V-VPAT records shall be maintained in a temperature-controlled environment. The temperature settings shall be maintained at a minimum of 50 degrees and a maximum of 80 degrees. V-VPAT records shall also be maintained in a dry environment, with storage at least 4 inches above the finished floor, for a period of 25 months following the election. The humidity of the environment shall not exceed 80% humidity for a period of more than 24 hours. V-VPAT records shall be stored in a manner that prevents exposure to light, except as necessary during recounts and audits.

e. Paper Ballots – Paper ballots shall be maintained in a dry, humidity-controlled environment. The humidity of the environment shall not exceed 80% humidity for a period of more than 24 hours. Additionally, paper ballots shall be stored at least 4 inches above the finished floor, for a period of 25 months following the election.

f. Video Data Records – Video data records shall be maintained in a dry, temperature-controlled environment. The humidity of the environment shall not exceed 80% humidity for a period of more than 24 hours. Temperature settings shall be maintained at a minimum of 40 degrees and a maximum of 80 degrees. Additionally, video data records shall be stored at least 4 inches above the finished floor, for a period of 25 months following the election.

4. Security Cameras or Other Surveillance

Unless otherwise instructed, continuous security camera recordings of specified areas shall be made beginning at least 90 days prior to the election and continuing through at least 30 days after the election. The following are the specific minimum requirements:

a. Counties over 50,000 registered voters shall make continuous security camera recordings of the following areas:

   i. All areas in which election software is used, including but not limited to programming, downloading memory cards, uploading memory cards, tallying results, and results reporting.

   ii. All areas used for processing absentee ballots, including but not limited to areas used for Signature Verification, tabulation, or storage of voted ballots.

   iii. The storage area for all voting equipment.

b. Counties under 50,000 registered voters shall make continuous security camera recordings of the following areas:

   i. All areas in which election software is used, including but not limited to programming, downloading memory cards, uploading memory cards, tallying results, and results reporting.

5. Equipment Maintenance Procedures

In addition to the requirements for voting systems specified in Election Rule 11, the following minimum standards shall be adhered to:

All equipment shall be stored throughout the year with serially-numbered, tamper-evident seals over the memory card slots for each device. The county shall maintain a log of the seals used for each device consistent to the logs used for tracking Election Day seals.

Equipment maintenance by the voting systems vendor for offsite repairs/replacements may be conducted outside of the dates from 120 days prior to the election and 60 days after any election in which the equipment is used. Counties may request from the Secretary of State a variance from this requirement in extreme situations. Upon such request, the Secretary of State shall respond to the request no later than 5 business days from receipt of the request.

For any equipment sent offsite for repairs or replacement, the county shall place a tamper evident seal over the memory card slots for the device after removal of all removable memory data. The county shall send a seal-tracking log under separate shipping to the vendor to verify and sign that the package has arrived with seals in place. Counties are required to keep a photocopy of this documentation with the voting device. To the extent possible with DRE devices, any archived election data maintained in memory banks shall be removed before shipping.

For equipment being sent to the vendor for offsite repairs/replacements, the county must maintain a log file for the device that shall contain the following: the model number, serial number, and the type of device; the firmware version; the software version (as applicable); date of submission to the vendor; name of the staff member(s) who packaged the device for shipment; seal number(s); applicable shipping information; and a photocopy of all documentation of communication between the county and vendor regarding the problem and remedy.

For equipment returning from the vendor after offsite repairs or replacements, the county shall attach to the log file the applicable shipping information, the date of return, name of the staff member(s) receiving the equipment, and the results of acceptance testing information.

For equipment receiving maintenance on-site by the vendor, the county shall conduct a CBI background check on all vendor personnel with access to any component of the voting system. CBI information shall be updated and maintained on file annually. Additionally, the vendor's representative shall be escorted at all times by a county employee while on-site. At no time shall the voting system vendor have access to any component of the voting system without supervision by a county employee.

Upon completion of any maintenance, the county shall conduct a full acceptance test of equipment that shall, at a minimum, include the Hardware Diagnostics test, as indicated in Rule 11, and conduct a mock election in which a county election official shall cast a minimum of ten (10) ballots on the device to ensure tabulation of votes is working correctly. All documentation of results of the acceptance testing shall be maintained on file with the specific device.

The Secretary of State shall be required to inspect the counties' maintenance records on a randomly selected 1% of all voting devices in possession of the counties throughout the state in even years, and to inspect the maintenance records on a randomly selected 5% of all voting devices in possession of the counties throughout the state in odd years.

6. Transportation of Equipment, Ballot Boxes, and Ballots

Counties are required to submit detailed plans to the Secretary of State prior to an election regarding the transportation of equipment and ballots both to remote voting sites and back to the central elections office or storage facility. While this may be handled in a multitude of methods, the following standards shall be followed when transporting voting equipment:

Delivery TO the Voting Location:

a. Transportation by County Personnel – County personnel shall at all times display a badge or other identification provided by the County. Two signatures and date of county personnel shall be required at the departure location verifying that the equipment, including memory card or cartridge, is sealed to prevent tampering. Upon delivery of equipment, at least two county elections personnel or Election Judges shall verify that all seals are intact and that the serial numbers on the seals agree with those on the seal-tracking log, and sign and date the seal-tracking log. If there is any evidence of possible tampering with a seal, or if the serial numbers do not agree, they shall immediately notify the County Clerk who shall follow the procedures specific to the incident as described in Section 10 of these security requirements.

b. Transportation by Election Judges – Election Judges that are receiving equipment from county personnel shall inspect all components of voting devices and verify the specific numbers by signature and date on the seal-tracking log for the device. The Election Judge receiving the equipment shall request two judges at the voting location to inspect the devices and to sign and date the seal-tracking log indicating that all seals are intact and that the serial numbers on the seals agree with those on the seal-tracking log. If there is any evidence of possible tampering with a seal, or if the serial numbers do not agree, they shall immediately notify the County Clerk who shall follow the procedures specific to the incident as described in Section 10 of these security requirements.

c. Transportation by Contract – Counties electing to contract the delivery of equipment to remote voting locations shall perform CBI background checks on the specific individuals who will be delivering the equipment. Additionally, the county shall ensure the security of equipment during transit by riding along with the delivery drivers, or following in a chase vehicle. Two county personnel shall verify, sign, and date the seal-tracking log upon release of the equipment and two county personnel shall verify, sign, and date the seal-tracking log upon acceptance of the equipment at the delivery point. If there is any evidence of possible tampering with a seal, or if the serial numbers do not agree, they shall immediately notify the County Clerk who shall follow the procedures specific to the incident as described in Section 10 of these security requirements.

Delivery FROM the Voting Location:

a. If memory cards or cartridges are to be removed from voting devices at remote voting locations, the following procedures are to be followed:

   i. Before removing a memory card or cartridge, two judges shall inspect and verify that all seals on the device are intact and that the serial numbers on the seals agree with those listed on the seal-tracking log. Both judges shall sign and date the seal-tracking log prior to breaking the seal. If there is any evidence of possible tampering with a seal, or if the serial numbers do not agree, they shall immediately notify the County Clerk who shall follow the procedures specific to the incident as described in Section 10 of these security requirements.
   ii. Judges shall place the cards or cartridges in a sealable transfer case that shall be sealed with two seals. Additional seal logs shall be maintained for the transfer case of the memory cards or cartridges.

   iii. Election judges shall place new seals over the empty memory card/cartridge slot and document the seal numbers used.

   iv. At least two judges shall accompany the transfer case containing the memory card/cartridge to the drop off location. Seal integrity and serial numbers will be verified, and logs will be signed and dated by county election officials receiving the equipment. If there is any evidence of possible tampering with a seal, or if the serial numbers do not agree, they shall immediately notify the County Clerk who shall follow the procedures specific to the incident as described in Section 10 of these security requirements.

v. County personnel or election judges transporting secured voting equipment must maintain chain of custody logs and seal-tracking logs. If there is any evidence of possible tampering with a seal, or if the serial numbers do not agree, they shall immediately notify the County Clerk who shall follow the procedures specific to the incident as described in Section 10 of these security requirements.

b. If devices are to be delivered with memory cards/cartridges intact, the following procedures shall be followed:

i. Two election judges shall verify that all seals are intact at the close of polls. Judges will sign the seal-tracking log with such indication. If there is any evidence of possible tampering with a seal, or if the serial numbers do not agree, they shall immediately notify the County Clerk who shall follow the procedures specific to the incident as described in Section 10 of these security requirements.

ii. At least two judges shall accompany the secured equipment to the drop-off location. Seals will be verified, and logs will be signed and dated by the county election official receiving the equipment. If there is any evidence of possible tampering with a seal, or if the serial numbers do not agree, they shall immediately notify the County Clerk who shall follow the procedures specific to the incident as described in Section 10 of these security requirements.

iii. Upon confirmation that the seals are intact and bear the correct numbers, the memory card or cartridge shall be removed and uploaded into the central count system.

iv. Election officials shall secure the equipment by placing a tamper-evident seal over the memory card slot and by updating the documentation to reflect the new seal numbers.

7. Emergency Contingency Plans for Voting Equipment and Voting Locations

All remote devices used in an election shall have sufficient battery backup for at least 2 hours of use. If this requirement is met by reliance on the internal battery of the voting device, then the clerk and recorder shall verify that all batteries are fully charged and in working order prior to the opening of polls at the voting location. This requirement also can be met with the purchase of third-party battery backup systems.

In the event of a serious or catastrophic equipment failure or equipment being removed from service at one or more polling locations, and if there is not adequate backup equipment to meet the requirements of Section 1-5-501, the county clerk shall contact the Secretary of State for authorization to use provisional ballots or absentee ballots as an emergency voting method.

8. Internal Controls for the Voting System

In addition to the access controls discussed in section 2 of this document, counties are required to change all passwords and limit access to the following areas:

a. Software – All software passwords shall be changed once per calendar year prior to the first election. This includes any boot or startup passwords in use, as well as any administrator and user passwords and remote device passwords.

b. Hardware – All hardware passwords shall be changed once per calendar year prior to the first election. This includes any encryption keys, key card tools, supervisor codes, poll worker passwords on smart cards, USB keys, tokens, and voting devices themselves as it applies to the specific system.

c. Password Management – A maximum of 2 county employees shall have access to passwords for all of the election software and hardware. Up to 10 people may have access to either the software or the hardware components of the voting system, but not both.

d. Internet Access – At no time shall any component of the voting system be connected, directly or indirectly, to the Internet.

e. Modem Transmission -- At no time shall any component of the voting system be connected to another device except for the vote tally software, directly or indirectly, by modem.

Remote sites may use modem functions of optical scanners and DREs only for the purpose of transmitting unofficial results, as permitted by the Secretary of State's certification documents for the specific systems. Counties using modem devices to transmit results shall meet the following requirements:

i. Transmissions may be used only for sending unofficial results; after all other steps have been taken to close the polls. All summary tapes should be printed before connecting any of the machines to a modem or telephone line.

ii. Modems cannot be used for any programming, setup, or individual ballot-casting transmissions.

iii. The receiving telephone number for the modem transmission shall be changed at least once per calendar year prior to the first election.

v. A maximum of 4 county employees shall be made aware of the telephone number receiving the transmission. Counties shall not publish or print the telephone number for any election judge. To the extent possible, the telephone number shall be programmed into the device and used by the device in a way that is hidden from election judges and voters from seeing the display of the number at any time.

f. Authorized County Personnel - Counties are required to include in their security plans the names and dates of CBI background checks for employees with access to any of the above areas or equipment. Each county shall maintain a storage-facility access log that details employee name, time, and purpose of access to the storage facility in which the software, hardware, or components of any voting system are maintained.

9. Security Training for Election Judges

Counties are required to include the details of their security training for their election judges, which shall include the time of training, location of training, and number of judges receiving the security training, as it applies to the following requirements:

a. In counties with more than 50,000 registered voters, in addition to any other training, the county shall conduct a separate training session for field technicians and election judges who will be responsible for overseeing the transportation and use of the voting systems, picking up supplies, and troubleshooting device problems throughout the Election Day.

b. In counties with fewer than 50,000 registered voters, the counties may include security training for field technicians and election judges who will be responsible for overseeing the transportation and use of the voting systems, picking up supplies, and troubleshooting device problems throughout the Election Day in the same class as normal training instruction for all election judges.

c. Security training shall include the following components:

i. Proper application and verification of seals and seal-tracking logs;

ii. How to detect tampering with voting equipment, memory cards/cartridges, or election data on the part of anyone coming in contact with voting equipment, including county personnel, other election judges, vendor personnel, or voters;

iii. How to detect suspicious behavior;

iv. Ensuring privacy in voting booths;

v. The nature of and reasons for the steps taken to mitigate the security vulnerabilities of DREs;

vi. V-VPAT requirements;

vii. Chain-of-custody requirements for voting equipment, memory cards/cartridges, and other election materials;

viii. Ballot security;

ix. Voter anonymity.

10. Remedies

If it is detected that the seal has been broken or if there is a discrepancy between the log and the serial number of either a voting device, or a memory card or cartridge, the condition must be confirmed by one or more of the remaining election judges for the location. The judges shall immediately notify the County Clerk, who shall investigate and determine appropriate action.

If the unit involved is a DRE, it must undergo a full manual reconciliation of the electronic votes cast and captured on the memory card against the paper audit record for that unit. If the unit involved is an optical scan device, it must undergo a full manual reconciliation of the counts in the memory card/cartridge against the paper ballots that were scanned by the unit. Specific requirements on the remedy are as follows:

If there is any evidence of possible tampering with a seal, or if the serial numbers do not agree, the County Clerk shall restore the chain of custody for the device and memory card in the following manner:

<u>If the evidence is prior to the start of voting:</u>

1. The device shall be sealed and securely delivered to the Clerk and Recorder.
2. If the seal is not over the memory card, the Clerk and Recorder shall reset the machine to pre-election mode, conduct hardware diagnostics testing as prescribed in Rule 11, and proceed to conduct a logic and accuracy test on the machine in full election mode, casting at least 25 ballots for counties with less than 50,000 registered voters, 50 ballots for counties with more than 50,000 registered voters on the device. The totals from the device shall be verified through the uploading process and determined to be accurate.
3. If the seal is over the memory card, the Clerk and Recorder shall remove the memory card, and insert a secured memory card into the device. The Clerk and Recorder shall conduct a hardware diagnostics test as prescribed in Rule 11, and proceed to conduct a logic and accuracy test on the machine in full election mode, casting at least 25 ballots for counties with less than 50,000 registered voters, 50 ballots for counties with more than 50,000 registered voters on the device. The totals from the device shall be verified through the uploading process and determined to be accurate.

4. Complete the necessary seal process and documentation to establish the chain of custody for the device and memory card.
5. Set the machine to election mode ready for a zero report.
6. At the conclusion of the election a full (all races) post-election audit shall be conducted on the device and results reported to the Secretary of State as required by Rule 11. This requirement is in addition to the random selection conducted by the Secretary of State.
7. Complete necessary reports for the Secretary of State regarding the incident.

If the evidence is after votes have been cast on the device but before the close of polls:

1. The device shall be sealed and securely delivered to the Clerk and Recorder.
2. The Clerk and Recorder shall close the election on that device, and perform a complete manual verification of the paper ballots (or V-VPAT Records) to the summary tape printed on the device that represents the record of votes on the memory card.
3. If the totals do not match then only the paper ballots (or V-VPAT Records) will be accepted in the official results for that device, and the device shall be re-sealed, secured and reported to the Secretary of State immediately - the device can no longer be used in the remainder of the election until the firmware and software on the device can be verified as directed by the Secretary of State.
4. If the totals match, the memory card may be uploaded into the tally software at the close of polls.
5. After verifying the totals, the paper ballots (or V-VPAT Records) and memory card shall be secured with seals and documented properly.
6. A new secured memory card shall be placed in the device. The Clerk and Recorder shall conduct a hardware diagnostics test as prescribed in Rule 11, and proceed to conduct a logic and accuracy test on the machine in full election mode, casting at least 25 ballots for counties with less than 50,000 registered voters, 50 ballots for counties with more than 50,000 registered voters on the device. The totals from the device shall be verified through the uploading process and determined to be accurate.
7. Complete the necessary seal process and documentation to establish the chain of custody for the device and memory card.
8. Set the machine to election mode ready for a zero report.
9. At the conclusion of the election a full (all races) post-election audit shall be conducted on the device and results reported to the Secretary of State as required by Rule 11. This requirement is in addition to the random selection conducted by the Secretary of State.
10. Complete necessary reports for the Secretary of State regarding the incident.

If the evidence is after the close of polls:

1. The device shall be sealed and securely delivered to the Clerk and Recorder.
2. The Clerk and Recorder shall perform a complete manual verification of the paper ballots (or V-VPAT Records) to the summary tape printed on the device that represents the record of votes on the memory card.
3. If the totals do not match then only the paper ballots (or V-VPAT Records) will be accepted in the official results for that device, and the device shall be re-sealed, secured and reported to the Secretary of State immediately - the device can no longer be used until the firmware and software on the device can be verified as directed by the Secretary of State.
4. If the totals match, the memory card may be uploaded into the tally software at the close of polls.
5. After verifying the totals, the paper ballots (or V-VPAT Records) and memory card shall be secured with seals and documented properly.
6. Complete the necessary seal process and documentation to establish the chain of custody for the device.
7. During the canvass process, a full (all races) post-election audit shall be conducted on the device and results reported to the Secretary of State as required by Rule 11. This requirement is in addition to the random selection conducted by the Secretary of State.
8. Complete necessary reports for the Secretary of State regarding the incident.

Prior to the submission of certified results from the county, the county clerk and recorder will provide a written report to the Secretary of State addressing the existence or absence of any security issues related to the implementation and operation of the voting system. All county documentation related to the voting system shall be available for inspection by the office of the Secretary of State for all devices used in the election.

11. Optional Physical Security Procedures

Any additional physical security procedures not discussed in these mandatory procedures shall be submitted to the Secretary of State for approval prior to the election.