

DIRECTIVE 2008-54

July 18, 2008

TO: ALL COUNTY BOARDS OF ELECTIONS WITH PREMIER DRE VOTING SYSTEM
RE: Direct Recording Electronic (DRE) Voting Machine Key Card Management

This Directive replaces Directive 2007-02 and the July 24, 2007 Memorandum regarding Direct Recording Electronic (DRE) voting machine key card management.

Premier's DRE voting machines use special security encryption, or "keys," on voting system access cards to perform management and voter functions. This relates to all four types of access cards: security, supervisor, administrator and voter access cards.

To ensure that the highest level of security for the election process is achieved, security encryptions on access cards should be changed prior to each primary and general election. However, boards of elections may choose to change security encryptions before every election, including special elections.

Management of security encryptions requires the use of special equipment that allows a user who has appropriate security access to change the key(s) on security, supervisor and administrator access cards. Changing the keys on these access cards also changes the passwords used to prevent unauthorized use of a DRE.

This directive addresses only the security encryption process for access cards. Boards of elections should also continue to observe all other recommended physical security requirements, security instructions and security processes related to voting systems.

Process

Keys on **voter access cards** must be changed by boards of elections staff through use of encoders.

Keys on **security, supervisor, and administrator access cards** must be changed by boards of elections utilizing one of the following three options:

1. If a board of elections has the necessary equipment, the persons assigned by the board may change the security encryptions on security, supervisor and administration access cards. The board must assign an even number of persons, with equal numbers from each major political party, to change security encryptions.
 - It is imperative that keys for access cards within a county are kept in sync (e.g., contain the same keys for DREs). Failure to do so will result in confusion and unusable cards at polling locations.
 - When the keys are changed, at least one board of elections employee from each political party shall witness the security encryption process and complete the appropriate form (**Form #KC 001**). The completed form shall be faxed to the secretary of state's office to the attention of:

Tom Sheridan, Project Specialist
(614) 752-4360 (fax)

2. A board of elections may schedule a day and time with one of the secretary of state IT regional liaison to appear at the board of elections office to change the security encryption on its security, supervisor and administration access cards. Please contact one of the IT regional liaisons directly to schedule a date for your county.
 - When the keys are changed by secretary of state IT regional liaisons, at least one board of elections employee from each political party shall witness the security encryption process and complete the appropriate form (**Form #KC 002**). The form shall be duplicated at the board for the board's records and the original delivered to the secretary of state's office by the IT regional liaison to the attention of Tom Sheridan, Project Specialist.
3. A board of elections may send its security, supervisor and administrator access cards, except those used for training purposes, to the secretary of state's office.
 - Cards should be bundled in groups of 20 for ease of counting.
 - Each board of elections must complete and submit an inventory control sheet (**Form #KC 003**) with the access cards. The inventory sheet and cards should be delivered or sent to:

Secretary of State's Office	or	Secretary of State's Office
Attn: Tom Sheridan		Attn: Tom Sheridan
Project Specialist		Project Specialist
180 E. Board St. 15 th Floor		P.O. Box 2828
Columbus, OH 43215		Columbus, OH 43216
 - Secretary of state staff will complete updates and/or changes to keys and will return the access cards to the county of origin on or before the write-in candidate filing deadline in order to allow counties time to use the access cards for logic and accuracy testing, as well as meet training needs.
 - New passwords will be communicated separately via the secure T-1 line to the secretary of state email account provided to the board of elections on the office workstation provided by the secretary of state.

When the security encryption is changed on security, supervisor and administrator access cards, the authorization code or "PIN" shall also be changed.

Keys on **voter access cards** are to be changed by boards of elections staff through use of the encoders located in the board office. This must be completed after keys and PINS on security, supervisor and administration access cards are changed utilizing one of the three outlined in this Directive.

Keys and PINS on DRE machines should be updated by using the updated security cards during logic and accuracy testing performed on each unit by the board of elections.

IMPORTANT POINTS TO REMEMBER

Training and Demonstration Voting Systems

Some DREs may be used for training and demonstration purposes. This equipment should be clearly labeled and kept separately from DREs used for elections. Before training and demonstration units can be utilized for an actual election, they must undergo logic and accuracy testing.

Supervisor and Administration Access Cards for Training and Demonstration Equipment

Supervisor and administrator access cards that are used for training staff, poll workers and the general public should be clearly labeled and kept separate from those used for elections. The security encryption on these cards should **not** be changed from the default setting of 111111 for ease of training.

Voter Access Cards for Training and Demonstration Equipment

Security encryption on voter access cards that are used for training staff, poll workers and the general public should be changed by boards of elections through use of the encoders at the board office.

Thank you for your assistance in complying with these important security practices

Sincerely,

Jennifer Brunner