

To: State Elections Board
From: Paul Malischke, representing Fair Elections Wisconsin
September 12, 2007

We urge you to approve the security recommendations with the following amendments.

Chapter EIBd 5 Ballot and Electronic Voting System Security

5.02 General Electronic Voting System Security Procedures

- (1) These procedures apply to all electronic voting equipment memory devices, including, but not limited to, prom packs, memory cards or any other removable memory devices that can be programmed or function to store and transfer ballot images or tabulation data. Memory devices for ballot marking terminals are included.
- (2) Throughout the life of the electronic voting system, the municipal clerk shall maintain control of all memory cards.
- (3) The municipal clerk shall keep a separate, perpetual, written chain-of-custody record for each memory card used with an electronic voting system.
- (4) Memory cards shall be stored securely at all times and each access and transfer shall be logged in the written chain-of-custody record.
- (5) With the agreement of the municipal clerk, the county clerk may store memory cards in secure location. Both clerks shall maintain separate, perpetual, written chain-of-custody records for each memory card used with an electronic voting system.
- (6) An additional written log shall record everyone who accesses the electronic voting system. This log shall include the name of the individual, the date and time the access begins, the purpose of the access, and the time the access ends.
- (7) Each memory card shall have or be assigned a unique and permanent serial number. If the memory card does not have a permanent and fixed serial number affixed by the manufacturer, a clerk shall if possible ~~may~~ affix a label to the cards which contains the clerk's original signature and a serial number.
- (8) The municipality shall use controlled, serialized seals that are tamper-resistant and resistant to inadvertent breakage along with a written log of all seals and associated serial numbers.
- (9) The municipal clerk shall maintain a written log that records which memory cards and serialized tamper-evident seals are assigned to particular voting stations or units.
- (10) The municipal shall maintain a written inventory of all keys that are used to gain access to electronic voting systems. The municipal clerk shall keep a perpetual, written chain-of-custody record for all such keys.

5.03 Pre-election procedures

- (1) The municipal clerk shall check the locks and security seals and compare to the logs to verify who accessed the electronic voting systems or memory cards since the previous election.
- (2) Memory cards shall be programmed to print a list of the software and firmware versions of the electronic voting system on each beginning-of-election-day zero report and end-of-day zero report. This information shall also be printed on any reports generated during the pre-election testing, including the public test, and the pre-recount public test conducted by the Board of Canvassers-

For electronic voting systems that cannot accommodate this requirement, this information ~~shall~~ may be recorded from the system start-up screen, either by municipal or county staff during the pre-election testing or by election inspectors during Election Day.

- (3) The records for both the pre-election test, ~~and~~ Election Day reports, and pre-recount public test conducted by the Board of Canvassers, must be maintained by the municipal clerk.
- (4) Except when necessary to program, test, or operate the system, each system must be closed and locked with a tamper-resistant seal which can be tracked using a unique and permanent serial number.
 - (a) Each input slot or access port, including USB, serial or modem ports, must be closed and locked using a tamper resistant seal which can be recorded using a unique and permanent serial number.
 - (b) Alternately, these slots or ports may be disabled, with written documentation of the dates and times maintained by the municipal clerk.
- (5) Any door by which access can be gained to the system controls must be closed and locked using a tamper-resistant seal which can be tracked using a unique and permanent serial number. The municipal clerk shall maintain a written record of such serial numbers.
- (6) Once a memory card is programmed for the election, it shall be immediately inserted into its assigned unit and sealed against unauthorized access with a serialized, tamper-evident seal which can be tracked using a unique and permanent serial number. The voting station shall not be set into election mode until after the memory card is sealed inside.
Alternately, memory cards may be locked in a secure location with controlled access; written documentation of access to programmed memory cards must be maintained.
- (7) The municipality or county shall obtain a signed “Certificate of Performance Compliance: Memory Card Security” from each vendor that provides voting systems, equipment, programming services, or memory cards to the municipality.
- (8) The municipality shall take reasonable precautions to assure the security of the equipment between the time it leaves possession of the clerk to be delivered to the polling place, and the time the chief inspector assumes possession at the polling place on election day.

5.04 Election day procedures

- (1) Before any ballots are cast on any unit, the integrity of the tamper-evident seals shall be verified by the chief election inspector before accessing compartments containing the memory card and unit power switch. The chief election inspector shall record this information on the Inspectors’ Statement (EB-104) and chain-of-custody document for the memory card.
- (2) Once the polls have opened, ballot removal from an optical scan machine or paper roll removal or replacement on a Direct Recording Electronic (DRE) machine shall be conducted with at least two election inspectors (or other sworn election team members appointed by the municipal clerk) present. The removal process, names of the election inspectors or sworn election team members, and time must be recorded on the Inspectors’ Statement (EB-104).
- (3) In post-election mode, election officials shall print the results report before breaking any seal (including but not limited to a seal covering a modem port), and before the removal of the memory card from the voting stations or units. If additional reports other than the results reports are available, these reports shall also be printed before the removal of the memory card.
After the results reports are printed, the serial numbers of all the security seals shall be recorded on the results report or Inspectors’ Statement (EB-104).
- (4) One copy of the results report and the memory cards shall be secured in a separate, sealed container or envelope by the chief election inspector. The chief election inspector and two additional election

inspectors shall sign their names across the seal of the secured envelope or container. The memory cards shall be promptly returned to the municipal clerk.

- (5) If results are transmitted by modem, the municipal clerk may access the memory card for transmission, but shall reseal and sign his or her name across the seal of the secured envelope or container. Before transmitting the results via modem, the clerk shall print an additional results report from the system and record the transmission time on the Inspectors' Statement (EB-104).
- (6) As an alternate procedure, the memory cards may remain sealed in the voting stations or units. The serial numbers of the security seals shall be recorded on the Inspectors' Statement (EB-104).

5.05 Post election procedures

- (1) After each election, the clerk responsible for storing the voting system shall conduct an inspection to ensure that each system is locked and secured. Written documentation shall note the date and time of the inspection and any applicable security seal numbers.
- (2) Before the next election or recount, the municipal clerk shall inspect the security seals to ensure that each seal number matches the initial ending documentation from the previous election. This inspection shall be documented in the written chain of custody record with time and date.
- (3) At each post-election meeting of the municipal Board of Canvassers, the members shall cross-check the log with the official results report or Inspector's Statement (EB-104). This shall be accomplished by comparing the serial numbers of the seals. The serial number(s) on the results report from the voting system shall be compared with the serial number of the seal(s) as recorded in the log during the pre-election testing. This check shall be carried out on five systems, or 10% of the total systems, whichever is greater. The county Board of Canvassers shall check ten systems. For a recount, all systems shall be checked. The ward numbers that are checked and the results shall be listed in the minutes of the meeting of the Board of Canvassers.

5.15 Alternate Security Procedures

- (1) The board recognizes the need for flexibility when implementing these procedures, and acknowledges that alternative means may be used to achieve and ensure an acceptable level of electronic voting equipment security.
- (2) The board will consider requests from municipalities and counties to implement alternative security procedures.
 - (a) The municipal clerk or county clerk shall submit a written request to implement alternative security procedures to the executive director of the board.
 - (b) The request shall describe the proposed security procedures in detail and include any documentation such as logs, flow charts and certification forms.
 - (c) The executive director of the board may approve the use of alternative security procedures for one election cycle.
 - (d) The board shall review all the approval of any alternative security procedures and may authorize continued use of the alternative security procedures.

EIBd 5.01 Ballot security. (1) Within the requirements of s. 7.51 (3), Stats., the terms “secure” and “seal” shall be interpreted together to mean that the ballots, within the container in which they are held, must be bound together in such a manner that no ballot may be removed, nor any ballot added, to the bound ballots without a visibly discernible and indelible record of or evidence of interference with or damage to that binding.

(2) Within the requirements of s. 7.51 (3) (a), Stats., a ballot container shall be considered “sealed” or “locked,” only if no ballot may be removed from the container or deposited into the container, and no other form of access to the bound ballots inside may be gained, without leaving visibly discernible and indelible evidence of, or record of, that entry or access into the container.

(a) Ballot bags shall be sealed with a serialized numbered seal that is tamper resistant, and the serial number recorded on the signed Ballot Container Certification (EB-101) attached to the bag. On election day, serial numbers of seals shall be recorded in the Inspector’s report (EB-104).

(b) Ballot boxes shall have all potential openings covered by an attached and signed Ballot Container Certification (EB-101).

(3) A ballot container shall not be considered “secured” unless it is stored in a room or other facility access to which is limited only to the clerk of the election district or to other persons known to the clerk, and access to which is not available to any other person.

After each election, the municipal Board of Canvassers shall verify that the ballot containers are sealed in accord with this rule. This shall include checking that the serial number on the seal of the ballot bag matches the number written on the EB-101). This check shall be carried out on five containers, or 10% of the total systems, whichever is greater. The county Board of Canvassers shall check ten containers. For a recount, all containers shall be checked. The ward numbers that are checked and the results shall be listed in the minutes of the meeting of the Board of Canvassers.

(4) Whenever the custodian of the ballots is required to open the ballot container and unseal the ballots – as part of a recount, an appeal of a recount, audit, or as part of a public records request under s. 19.35, Stats. – before opening the ballot container the custodian shall make a record of whether the container is sealed in accord with this rule, and shall record the serialized number of the seal. The custodian shall make a record of that entry, and of that ballot review. Upon completion of the review of the ballots, the custodian shall re-secure them in the manner provided in s. 7.51, Stats., unless destruction is authorized under s. 7.23, Stats.

(5) Security of the ballots and the ballot container shall be maintained as provided under s. 7.51, Stats., until destruction of the ballots is conducted under s. 7.23, Stats. Destruction of the ballots under s. 7.23, Stats., requires shredding, incineration, or some other form of obliteration of the ballots.

History: Cr. Register, January, 1992, No. 433, eff. 2–1–92.