

NOTICE OF PROPOSED RULE: GAB CH. 5

GOVERNMENT ACCOUNTABILITY BOARD

NOTICE IS HEREBY GIVEN that pursuant to ss.5.05(1)(f), 5.93, and 227.11(2)(a), Stats., and interpreting ss.5.84, 5.86, 5.87, 5.90, 5.905, 5.91, 7.23, 7.51, and 9.01 Stats., and according to the procedure set forth in s.227.16(2)(e), Stats., the State of Wisconsin Government Accountability Board will adopt the following rule as proposed in this notice without public hearing unless within 30 days after publication of this notice, the Board is petitioned for a public hearing by 25 persons who will be affected by the rule; by a municipality which will be affected by the rule; or by an association which is representative of a farm, labor, business, or professional group which will be affected by the rule.

ANALYSIS PREPARED BY GOVERNMENT ACCOUNTABILITY BOARD:

1. Statutory authority: ss.5.05(1)(f), 5.93 and 227.11(2)(a).
2. Statutes interpreted: ss.5.84, 5.86, 5.87, 5.90, 5.905, 5.91, 7.23, 7.51, and 9.01, Stats.
3. Explanation of agency authority: The Government Accountability Board's rule on ballot security, under ss.7.23 and 7.51, Stats., has become outdated because of advances in technology and because of heightened administrative and public concerns about ballot security in light of recent security and chain-of-custody problems in elections both in Wisconsin and in other states. To address those concerns and to update ballot security in Wisconsin, the Board proposes to repeal and re-create chapter GAB 5, the ballot security rule.
4. Related statute(s) or rule(s): ss.5.66, 5.85, 5.86, 5.87, 5.90, 7.10, 7.15, 7.24, 7.37, 7.53, 9.01, and 12.13, Stats.
5. Plain language analysis: The proposed rule provides the requirements for maintaining the security of ballots that are cast at an election and maintaining the integrity of the tabulation of those ballots in the canvass of an election.
6. Summary of, and comparison with, existing or proposed federal regulations: Federal law does not apply to the preparation, printing, or security of ballots. Federal law does require that materials, including ballots, relating to any election in which a federal office is on the ballot, must be preserved for not fewer than 22 months.

7. Comparison with rules in adjacent states: Illinois, Iowa, Michigan, and Minnesota all statutorily require that after ballots have been counted, they shall be secured in a sealed envelope or other container in such a manner that no ballot may be removed without breaking the seal on that container. The ballots and other election documents in those sealed containers are returned to the custody of the local election official who will hold them until they may be destroyed under state and federal law.

Generally, unlike Wisconsin's rule, the law in all four states provides for the retention of unused ballots until destruction of all ballots is authorized by state and federal law.

8. Summary of factual data and analytical methodologies: Adoption of the rule was predicated on federal and state mandate rather than on any factual data or analytical methodology.

9. Analysis and supporting documents used to determine effect on small business or in preparation of economic impact report: The rule will have no effect on small business, nor any economic impact.

10. Effect on small business: The creation of this rule does not affect business.

11. Agency contact person (including e-mail and telephone): George A. Dunst, Staff Counsel, Government Accountability Board, 17 West Main Street, P.O. Box 2973, Madison, Wisconsin 53701-2973; Phone 266-0136; george.dunst@wisconsin.gov

12. Place where comments are to be submitted and deadline for submission:
Government Accountability Board, 17 West Main Street, P.O. Box 2973, Madison, WI 53701-2973; (elections.state.wi.us)

Pursuant to the authority vested in the State of Wisconsin Government Accountability Board by ss.5.05(1)(f) and 227.11(2)(a), Stats., the Government Accountability Board proposes an order to repeal and re-create Chapter GAB 5, relating to ballot security, and interpreting ss.5.84, 5.86, 5.87, 5.90, 5.905, 5.91, 7.23, 7.51, and 9.01, Stats.

SECTION 1. Chapter GAB 5 is repealed and re-created to read:

Chapter GAB 5

Ballot and Electronic Voting System Security

GAB 5.01 Ballot security. (1) In this section:

- (a) “Board” means the government accountability board.
 - (b) “Certificate of performance compliance” means the document provided by voting equipment vendors certifying that the equipment complies with the performance requirements of s.5.91, Stats.
 - (c) “Chain-of-custody” means the recorded movement and location of election ballots from the time of delivery of the ballots to the municipal clerk or board of election commissioners until the destruction of the ballots is authorized under s.7.23, Stats.
 - (d) “Custodian” means the election official who is authorized by chs. 5 to 12 to take possession and control of the ballots from the time of delivery of the ballots to the clerk or board of election commissioners until destruction of the ballots is authorized under s.7.23, Stats.
 - (e) “Electronic voting system” has the meaning given in s.5.02(4m), Stats.
 - (f) “Firmware” means the computer software stored in read-only memory or programmable read-only memory.
 - (g) “Modem” means a device for transmitting data between two computers over telephone or other communication lines.
 - (h) “Results report” means the print-out of voting data by a piece of electronic voting equipment.
 - (f) “Software” has the meaning given in s.5.905(1), Stats.
- (2) Within the requirements of s.7.51(3), Stats., the terms “secure” and “seal” shall be interpreted together to mean that the voted ballot container must be closed in such a manner that no ballot may be removed, nor any ballot added, without visible evidence of interference or damage to the ballot container.
- (3) Within the requirements of s.7.51(3) (a), Stats., a ballot container shall be considered “sealed” or “locked,” only if no voted ballot may be removed from or deposited into the container, and no other form of access to the ballots inside may be gained without leaving visible evidence of that entry or access into the container.

Ballot bags shall be sealed with a tamper-evident, serialized numbered seal. The serial number shall be recorded on the signed ballot container certification (EB-101) attached to the

bag. Serial numbers of the seals also shall be recorded on the Inspectors' Statement (EB-104). Ballot boxes or containers shall have all potential openings secured in such a manner that no ballot may be removed, nor any ballot added, without visible evidence of interference or damage to that ballot container. Ballot boxes or containers shall have attached a signed ballot container certification (EB-101).

- (4) A sealed ballot container shall not be considered "secured" unless it is stored in a manner in which access to the container is limited only to the clerk of the election district, board of election commissioners, or to persons authorized by the clerk or the board of election commissioners, and access to which is not available to any other person.
- (5) Whenever the custodian is required to open the ballot container and unseal the ballots as part of a central count proceeding under s.5.86, Stats., board of canvass proceeding under Ch. 7, Stats., audit of electronic voting equipment after an election under s.7.08(6), Stats., recount or an appeal of a recount under s.9.01, Stats., or as part of a public records request under s.19.35, Stats., before opening the container the custodian shall record in the minutes of the proceeding whether the container is sealed and shall record the serialized number of the seal. The custodian shall make a record of the entry and of the ballot review. Upon completion of the review, the custodian shall re-secure them in the manner provided in s. 7.51, Stats., unless destruction is authorized under s. 7.23, Stats.
- (6) 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 authorized under s. 7.23, Stats., requires shredding, incineration, or some other form of obliteration of the ballots.
- (7) At the time of a recount, the serial numbers on the seals of the ballot container shall be compared with the serial numbers written on the signed ballot container certification (EB-101). All containers shall be compared in a recount. The ward numbers and the results of the serial number verification shall be recorded in the minutes of the recount.
- (8) The municipal clerk or board of election commissioners shall securely maintain all ballots from the time of receipt from the printer or county clerk through delivery to the polling place.

5.02 General Electronic Voting System Security Procedures

- (1) These procedures apply to all electronic tabulating voting equipment memory devices, including prom packs, memory cards, or any other removable memory devices that can be programmed or functioned to store and transfer ballot images or tabulation data.
- (2) Throughout the life of the electronic voting system, the municipal or county clerk shall maintain control of all memory devices in a secure manner at all times. With the agreement of the municipal clerk or board of election commissioners, the county clerk or county board of election commissioners may store memory devices in a secure location. The municipal

clerk or board of election commissioners shall secure all keys to the electronic voting equipment.

- (3) For each election, there shall be a separate, written chain-of-custody record for each programmed memory device used with an electronic voting system. Each transfer shall be logged in the written chain-of-custody record.
- (4) Each programmed memory device shall have or be assigned a unique and permanent serial number. If the memory device does not have a permanent serial number affixed by the manufacturer, a clerk shall, if possible, affix to the device a serial number or unique identifier.
- (5) The municipality shall use controlled, serialized seals that are tamper-evident and resistant to accidental breakage along with a written record of all seals and associated serial numbers.
- (6) For each election, the municipal clerk shall record on the Inspectors' Statement (EB-104), which memory devices and which serialized tamper-evident seals are assigned to particular voting stations or units.

5.03 Pre-election procedures

- (1) The clerk who has possession of the electronic voting systems or memory devices shall ensure that the equipment and memory devices have been secured properly since the previous election.
- (2) Memory devices 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 under s.5.84(2), Stats.

For electronic voting systems that cannot accommodate this requirement, the software and firmware information shall be recorded from the system start-up screen, either by municipal or county staff during the pre-election testing under s.5.84(1), Stats., or by election inspectors on Election Day under s.5.84(2), Stats.

- (3) The records for the pre-election test under s.5.84, Stats., pre-recount test under s.5.90, Stats., and Election Day reports under ss.7.51 and 7.53, Stats., must be maintained by the appropriate clerk or board of election commissioners.
- (4) Except when necessary to program, test, or operate the electronic voting and/or programming equipment, any point by which access can be gained to the system controls must be closed and locked or secured with a tamper-evident seal that can be tracked using a unique and permanent serial number. The appropriate clerk shall maintain a written record of the serial numbers required by this subsection.

- (5) After a memory device is programmed, tested, and delivered to the municipal clerk for the election, it shall be immediately and continuously maintained in a secure location with controlled access limited only to users authorized by the clerk or board of election commissioners.

Upon insertion of a memory device into its assigned unit, it shall be sealed against unauthorized access with a serialized, tamper-evident seal that can be tracked using a unique and permanent serial number. The municipal clerk or board of election commissioners shall record the serial numbers on the Inspectors' Statement (EB-104).

- (6) When applicable, for each election the municipal or county clerk or board of election commissioners shall obtain a signed "Certificate of Performance Compliance: Memory Device Security" from each voting equipment manufacturer that provides programming services or memory devices to the municipality or county.
- (7) The municipality shall take reasonable precautions to ensure the security of the equipment between the time it leaves the possession of the clerk or board of election commissioners 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 piece of voting equipment, the integrity of the tamper-evident seals shall be verified by the chief election inspector verifying that the tamper-evident seal serial number on the Inspectors' Statement (EB-104) matches the tamper-evident seal serial number contained on the electronic voting equipment. Any irregularity or discrepancy between the two numbers shall be reconciled before using the equipment.
- (2) After 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 or board of election commissioners) present. The removal process, the names of the election inspectors or sworn election team members, and the time of removal must be recorded on the Inspectors' Statement (EB-104).
- (3) After the polls have closed, election officials shall print a results report before breaking any seal on the equipment and before the removal of the memory device from any piece of voting equipment. If additional reports other than the results reports are required, these reports shall also be printed before breaking any seal on the equipment and before the removal of the memory device.
- (4) The chief election inspector shall compare the serial numbers of all security seals, then verify by initialing the Inspectors' Statement (EB-104). Any additional seals used during the election must also be recorded on the Inspectors' Statement (EB-104).

- (5) The memory device shall be secured in a separate, tamper-evident sealed container or envelope by the chief election inspector. The memory devices shall be promptly returned to the municipal or county clerk or board of election commissioners.
- (6) If vote results are transmitted by modem, the municipal clerk or board of election commissioners may access the memory device for transmission of those results, but shall reseal the memory device in a secured envelope or container.
- (7) If removal of the memory device is not required, the device may remain sealed in the voting equipment. The serial numbers of the security seals shall be verified and initialed on the Inspectors' Statement (EB-104).

5.05 Post election procedures

- (1) After each election, the clerk or board of election commissioners responsible for storing the voting equipment shall conduct an inspection to ensure all system access points are closed, locked, and secured.
- (2) At each post-election meeting of the municipal board of canvassers, the members shall verify that the tamper-evident serial numbers from the voting equipment have been recorded on five Inspectors' Statements (EB-104) or 10% (whichever is greater) of the total statements, and have been initialed by the Chief Election Inspector. The county board of canvassers shall verify ten Inspectors' Statements. All Inspectors' Statements (EB-104) shall be verified by the appropriate board of canvassers in a recount. Proper documentation shall be maintained.

5.15 Alternate Security Procedures

- (1) The Government Accountability 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 counties to implement alternative security procedures.
 - (a) The county clerk, or the municipal clerk or board of election commissioners through the county clerk or county board of election commissioners, shall submit a written request to implement alternative security procedures to the Board's director and general counsel.
 - (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 director and general counsel may approve the use of alternative security procedures for one election cycle.

- (d) The Board shall review the director and general counsel's approval of any alternative security procedures and may authorize continued use of those procedures.

INITIAL REGULATORY FLEXIBILITY ANALYSIS:

The creation of this rule does not affect business.

FISCAL ESTIMATE:

The creation of this rule has no fiscal effect.

CONTACT PERSON:

George A. Dunst
Staff Counsel, Government Accountability Board
17 West Main Street, P.O. Box 2973
Madison, Wisconsin 53701-2973; Phone 266-0136

The creation of this rule will take effect on the first day of the month following its publication in the Wisconsin Administrative Register pursuant to s.227.22(2), Stats.

Dated July 31, 2008

KEVIN J. KENNEDY
Director and General Counsel
Government Accountability Board