

Date: May 5, 2008

To: Members of the Government Accountability Board

From: Paul Malischke

Subject: Security rule ElBd 5 draft dated April 24, 2008
Agenda Item I

The following issues need to be addressed before the rule is approved.

1) Election Management Systems

There is nothing in the rule about this crucial part of the election system. According to the EAC glossary, such a system “defines, develops and maintains election databases, performs election definitions and setup functions, format ballots, count votes, consolidates and report results, and maintains audit trails.”

The Iowa rule 22.50(2) states that computers used in the election administrator’s office to prepare ballots and voting equipment programs or to compile and report election results should not be used for any other function and should not be linked to any computer network or to the Internet. Instead, data can be safely transferred to the Internet from the Election Management System in other ways, e.g., by using write-once media such as a CD ROM and a web server.

2) Audits by GAB staff

There is nothing in the rule about regular compliance reviews by GAB staff. Let’s avoid the embarrassing situation that developed with accessibility of polling places, where it took an outside audit to ensure compliance. Add the following to the rule:

- GAB staff shall audit the EB-106 (Board of Canvassers) forms for the inspection in 5.05 (2).
- GAB staff shall review the minutes of recounts to determine if the rule is being followed.
- GAB staff shall make field inspections to monitor compliance at poll closings, Board of Canvassers meetings, and recounts.
- GAB staff shall provide a midyear annual report to the Board on the extent and results of their auditing of whether the security requirements are being followed, and all follow-up actions if they are not being followed.

3) Security for electronic ballot boxes

The draft establishes a weaker level of security for electronic ballot boxes (memory devices) than for ballot bags during the time they are between the polling place and the clerk's office. During this time, 5.01(2) specifies that the ballots bags must have a serialized seal and the number recorded.

5.04 (5) should be changed to specify this same level of security for the memory cards during this critical time.

4) Keep records of seal numbers separate from the seals

In order for a system of numbered seals to provide optimum security, the record of the numbers should be kept separate from the actual seals. Adherence to this basic principle can be improved in 5.01 (6) and 5.03 (5) as follows.

5.01 (6) The draft states that at the time of a recount, the serial numbers of the seals on all ballot bags shall be compared to the seal number written on the attached ballot container certificates (EB-101).

This should be changed so that the ballot bag seal's serial number is compared to the number logged on the EB-104 inspectors report as required by 5.01(2). It is more likely that the inspector's report is stored separately from the ballot bag. The best practice would be to compare both records (EB-104 and EB-101) and with the actual seal.

5.03 (5) allows a situation where one person (the chief inspector) might have both the sealed equipment and the log of the seal number (EB-104).

The draft should be changed to add that the serial number shall also be written in a log maintained by the clerk. Consider adding back from the January 28th draft 5.02(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."

5) Seal all electronic access ports

The draft deletes 5.03 (4)(a) of the draft presented at the January 28 GAB meeting. This section should be restored. "Each electronic 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 serial number. The municipal clerk shall maintain a written record of such serial numbers." A voting machine is not secure unless all electronic access ports are secure.

A recent report from the University of Connecticut Department of Computer Science demonstrated that malicious software could be installed on a voting machine through the serial port. See <http://www.acsac.org/2007/papers/159.pdf>, section 3.3.