

Date: November 11, 2008
To: Government Accountability Board
From: Paul Malischke malischke@yahoo.com

Subject: Administrative Rule Chapter 5
Ballot and Electronic Voting System Security

The integrity of our elections depends upon having a solid security rule and ensuring that it is being followed.

The importance of security of ballots is obvious, particularly for voted ballots. If there is a recount or an audit of the vote count, we want to be certain that the ballots we are recounting are the ones actually marked by the voters.

The security of our voting equipment and software has also become critical, to avoid damage or corruption. Detailed studies have found severe vulnerabilities in voting equipment systems. Prominent studies have been conducted by the Secretary of State of California (“Top to Bottom Review”), and by the Secretary of State of Ohio (“EVEREST”).

The vulnerability of voting systems was summed up on page 2 of a report supported by a National Science Foundation grant to A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE), dated May 5, 2008:

“Of course, numerous studies have shown that currently deployed voting systems are susceptible to undetectable malicious attacks. The voting systems produced by all four manufacturers with significant market share in the United States have been subjected to thorough batteries of adversarial testing, source code review, accessibility testing and documentation review. All of these systems have vulnerabilities that could relatively easily be exploited to alter the results of an election. These studies demonstrate that individual vote-capture devices as well as central-count systems are susceptible to attacks that could lead to undetected changes in election results.”

Security is only as good as the weakest link. The proposed rule not only has weak links, it has missing links.

Major flaws in the proposed rule are:

1. No security requirements for computerized Election Management Systems
2. No requirements to seal electronic access ports
3. No separate clerk’s record kept of the serial numbers of security seals for the memory cards
4. No compliance monitoring

In a letter from Kevin Kennedy to Kenosha County Supervisor Jennifer Jackson, dated May 2, 2008, Mr. Kennedy describes this goal: “to ensure the voting equipment used in Wisconsin is secure and the public can readily verify that local election officials are following the rules and procedures established to ensure secure, accurate, and transparent elections.”

In order to attain this goal, the weak and missing security links must be rectified.

1) Election Management Systems

There is nothing in the current rule about this key component of the election system. According to the US Election Assistance Commission (EAC) glossary, an Election Management System “defines, develops and maintains election databases, performs election definitions and setup functions, formats ballots, counts votes, consolidates and reports results, and maintains audit trails.”

In a nutshell, one computer tells every voting device in the jurisdiction how to read and tally ballots, and then consolidates the totals. Therefore, corruption of the election management system is tantamount to corrupting every voting device in the jurisdiction.

Certainly, the security of the software and hardware of election management systems is crucial. Oddly, the rule completely ignores election management systems. The rule must be modified to include comprehensive security for election managements systems, including but not limited to the following.

- Require that all equipment, including election management systems, never be connected to the Internet. This would mean that a dedicated computer be used for running election management system software, and communication to outside systems be accomplished by transferring data using secure one-way media such as a CD-R.
- Include the recommendation of the EAC regarding dedicating the computer to this purpose only.
- Include rules on passwords and restricting access to people authorized by the clerk. (See Iowa rule 721—22.50(52))

The preface to the proposed rule as printed in the Administrative Register has a section on comparison with rules in other states. However, the comparison provided only pertains to section 5.01 of the rule, which deals with ballot security. The Administrative Register does **not** contain a description of comparison for the sections dealing with electronic voting systems, sections 5.02, 5.03, 5.04, and 5.05. This is surprising, since the rule promulgation procedure requires comparison. Below is some information from the US Election Assistance Commission (EAC), the League of Women Voters, the Election Technology Council, and other states.

EAC

The federal Election Assistance Commission was explicitly set up by Congress to provide assistance with developing these types of rules.

Page one of the EAC 2006 “Quick Start Management Guide for Voting System Security” states: “Do not allow any software on your vote tabulating computer except the voting system software itself. Specifically, do not allow office automation software, such as Microsoft® Word, PowerPoint, and Excel, or networking software, such as e-mail and network browsers. Verify that your voting system is not connected to any network outside the direct control of the election office.”

US League of Women Voters “Safeguarding the Vote”

“In the debate over the vulnerability of electronic systems to hacking and software tampering, critics have cited the danger of viruses and hacking. Election officials can reduce this risk by maintaining the system in isolation. In other words, no component of the system should ever be connected to the Internet.”

Election Technology Council (a trade association consisting of vendors of voting systems) From “Safeguarding the Vote: Applying Best Practices to Mitigate Perceived Threats for Voting Systems” <http://www.electiontech.org/documents/SafeguardingtheVotepracticesETCfinal.pdf> This document discusses the threat of external entry in to the central tabulation computer. “This threat is easily countered through the **adoption of state and/or local requirements** that tabulation computers are **not connected to the Internet** or any open network at any time, and by assuring that the physical and procedural security of the Central Tabulation Center is maintained at all times. For reporting of election results on election evening, the common practice of exporting the unofficial cumulative report summaries to an external device for transfer and subsequent upload to the Internet removes this threat in its entirety.” Also, see the last sentence of the attached Premier Election Solutions Product Advisory Notice, dated May 29, 2008.

Iowa Administrative rule Chapter 22, page 18

22.50(2) Computers. For security purposes, computers used in the commissioner’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.

Minnesota 206.845 BALLOT RECORDING AND COUNTING SECURITY.

Subdivision 1. **Prohibited connections.** The county auditor and municipal clerk must secure ballot recording and tabulating systems physically and electronically against unauthorized access. Except for wired connections within the polling place, ballot recording and tabulating systems must not be connected to or operated on, directly or indirectly, any electronic network, including a local area network, a wide-area network, the Internet, or the World Wide Web. Wireless communications may not be used in any way in a vote recording or vote tabulating system. Wireless, device-to-device capability is not permitted. No connection by modem is permitted. Transfer of information from the ballot recording or tabulating system to another system for network distribution or broadcast must be made by disk, tape, or other physical means of communication, other than direct or indirect electronic connection of the vote recording or vote tabulating system.

Alaska

State of Alaska, Division of Elections AccuVote Security Enhancements and Features (2007): “Ensure that no GEMS computer is connected to a network or the Internet and do not allow any software on the GEMS computer except for the voting system software itself. Use only the GEMS computer for programming an election.” A 2008 study by the University of Alaska, appendix D, reaffirmed and strengthened this. (GEMS = Global Election Management System.)

Arizona

In a letter dated June 5, 2008, Secretary of State Jan Brewer writes that Arizona has twenty-five security laws and procedures, including:

- “Requiring all election management software and equipment to stand alone and not be attached to any other computer or the Internet.”
- “Requiring election equipment firmware and software hash codes be verified against the National Institute of Science and Technology database before each election to assure the integrity of the software used at every election.”
- “Prohibiting the use of wireless communication.”

Georgia 183-1-12-.02

“No other software shall be loaded onto or maintained or used on computers on which the GEMS software is located except as specifically authorized by the Secretary of State.” This section also imposes requirements on physical access to the systems.

California Section 19217 of their statutes reads:

“No voting system or part of a voting system shall be connected to the Internet at any time.”

“(c) No voting system or part of a voting system shall receive or transmit wireless communications or wireless data transfers.”

Florida From the Florida Department of State, Donald Palmer, Director of Elections, to local supervisors of elections, dated June 3, 2008

“...maintain your Election Management System’s integrity by applying the following long-standing best practices.

“1. Secure Location. Make sure to install all secure systems in a protected location where only authorized personal are allowed.

“2. Enforce a password policy. A comprehensive policy should be utilized to prevent any unauthorized access and log authorized access. This should include a timeout feature to lock the terminal after a period of non-use.

“3. Turn off and remove unneeded services. The secure voting system should, by default, have unnecessary application or operating system services disabled or removed.

“4. Air-gapping the system. Continue to ensure that the system has **no outside network access**, wired or wireless, through the system’s communication ports. Communication between the secure voting system and outside systems, such as the transfer of audio files, should be executed on secure one-way media.

“5. Less secure to secure environment communication. Communication between an outside system and the secure voting system environment should be executed with the utmost care. Only authorized and verifiable safe files should be resident on any removable media connected to the secure environment.

“6. Secure to less secure environment communication. When any secure, protected, or sensitive information is passed from a secure to less secure environment it should be protected with encryption, if possible. This ensures that the data maintains its integrity and anonymity when outside of the secure environment. Secure data should not be operated on or manipulated outside of a secured environment.

“7. Installation of software. A secure system should only be subjected to authorized and verified software installations. This means that software to be installed should originate from a reputable vendor and verified by matching its digital signature with that published by the vendor. Other software installations should be deemed insecure and should not be introduced into the secure system.”

2) Seal all electronic access ports on the voting machines

The proposed rule deleted a paragraph previously approved by the State Elections Board in 2006 that sealed against other methods of attacking a voting machine. 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.

- The following should be added back into the rule. This was section 5.03 (4)(a) of the draft presented at the January 28, 2008 GAB meeting. “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.”

If it is not possible for some existing equipment to comply, counties may apply for alternate security procedures per section 5.15 of the proposed rule.

Why is this important? The end-of-day printout is used by the Board of Canvassers to certify the election. The voting machine must be kept isolated from electronic communication, including modem connection, until that record is printed.

EAC Page one of the EAC 2006 “Quick Start Management Guide for Voting System Security” states: “All unused connections on the voting systems should be sealed, including universal serial bus (USB), parallel, and other ports.”

Election Technology Council From “Safeguarding the Vote”, as described above, page 4 “In addition, sealing those ports on the units which are not relevant to the voting process will provide another layer of protection...”

3) Keep a record of seal numbers separate from the seals

In order for a system of numbered seals to provide optimum security, a record of the numbers should be kept separate from the actual seals. Keeping them separate makes it more difficult to successfully tamper with the seal and the record. This is accomplished in section 5.03 (4), but it is skipped in 5.03 (5), second paragraph.

This section deals with the seal over the memory card in the voting machine. 5.03 (5) states “The municipal clerk or board of election commissioners shall record the serial numbers on the Inspector’s Statement (EB-104).” This allows a situation where one person (the chief inspector) might have possession of both the sealed equipment and the only log of the seal number.

- The rule should be changed to include that the serial number shall **also** be written in a log maintained by the clerk. Add this wording to the bottom of 5.03 (5): “The appropriate clerk shall maintain a written record of the serial numbers required by this subsection.” This is the same wording already in the previous section.

