

Subject: NJ examination hearing for Sequoia WinEDS 3.1.073
From: Rebecca Mercuri and Irene Goldman
Date: October 5, 2006

On September 29, 2006, the New Jersey Division of Elections conducted an “examination hearing” of the Sequoia Voting Systems WinEDS Election Database Software Version 3.1.073, in Trenton at the 44 S. Clinton facility. The session was announced as a “Public Hearing on Voting Machines” on September 26 via an email from the NJ Office of the Attorney General. In attendance were officials from about a third of the NJ counties, two representatives from the public (Rebecca Mercuri of Notable Software, Inc. and Irene Goldman of the Coalition for Peace Action), the press (New Jersey Network News, who filmed the entire hearing and broadcast a segment about it in that evening’s news, and the Star Ledger), and various state offices (election-related staff from the Attorney General’s Office and the NJ Division of Elections). The session was chaired by Richard Woodbridge (a patent attorney), along with Daryl Mahoney (a Bergen County election official) and John Fleming (computer manager from the Attorney General’s office), forming the examination panel. Representatives from Sequoia, Ken Lanis (product specialist) and Christina Valeriano (marketing), presented the updated WinEDS software for certification.

Richard Woodbridge opened the session by announcing that there would be no participation of the audience during the two-part evaluation, and that there would be a 10-minute break between the parts, as is their custom. Part One would consist of a presentation by the Sequoia representatives. Part Two would involve a step-by-step review of the presentation according to NJ Title 19. When asked about this, the Sequoia representatives mentioned that they were not really familiar with the Title 19 requirements, nor did they have copies with them. Portions of the state code, namely 19:48-1, 19:48-2, 19:48-3, 19:53A-3, 19:53A-4, and 19:53A-5, were provided to the public and the Sequoia reps as paper copies, by the Attorney General’s Office. Sequoia Voting Systems provided everyone in attendance with copies of their “WinEDS for AVC Edge/Advantage Change Release Summary” pamphlet, Release 3.1, Document Version 1.06, September 2006, Part Number 089352411, which was marked “Confidential and Proprietary” on all pages.

The demonstration was conducted using a PC-laptop running a Microsoft Windows operating system. Cartridge programming hardware was connected to the laptop via cables. Two Sequoia Advantage AVC voting machines were in the room, but were not used.

Ken Lanis first went through a discussion of the updated features of the new WinEDS software. These were characterized as “bug fixes” and “enhancements.” Many of the new features pertained to the ability to more easily construct the ballot layout and provide a variety of end-of-day reports. The use of more natural-sounding speech synthesis modules via the Microsoft Operating System had been added in order to eliminate the need for individual voice recordings for the ballot items in the accessibility module, and problems that caused the audio not to be synchronized with all items on the ballot are supposed to have been corrected. Following the verbal description, some of the new features were demonstrated and a ballot cartridge was programmed. The examination panel did not think it was necessary to see whether the cartridge actually worked in the

voting machines as intended, nor did the panel appear to have checked to see if all bugs that have been experienced by NJ counties have actually been corrected.

Following the demonstration, the examination panel made a determination of whether the modifications constituted an “improvement or change which does not impair its accuracy, efficiency, or ability to meet such requirements” (as per Title 19, 19:53A-3 and A-4). The three panel members were polled and all stated their belief that since the update “did not deal with the voting machine itself” “in terms of its functionality” the reexamination or reapproval was unnecessary, under the conditions of the State law. They reserved their opinion to be published at a later date (in about a week), and also allowed that this determination did not prevent other questions from being asked.

Panelist John Fleming asked a number of questions with regard to the disclosure that the new software allowed for posting of election night reports directly to the Internet via FTP, a Web server, or email messages. Fleming was concerned with the fact that such connectivity was even allowed at all and also whether any municipalities had been connecting their election systems to an open network. Ken Lanis informed him that some counties do that, to which Fleming replied, “that’s a scary thought.” The panel also asked some questions regarding the type of cryptography used in the system, which were not able to be answered by the Sequoia representatives.

Rebecca Mercuri was then permitted to ask a number of questions, many of which were not able to be answered by the examination panel or the Sequoia representatives. These were as follows (somewhat paraphrased here):

Q: It is understood that components of voting equipment may receive 2002 federal certification, even though the entire system is not federally certified at that level. What is the case for the Sequoia system WinEDS software?

A: The version of WinEDS that is being submitted to NJ has been 2002 certified by the Cyber lab. Further information would be provided regarding whether the entire system is 2002 or just 1990 compliant.

Q: There appears to be no indication on the NIST website that the current WinEDS build has been escrowed in their digital signature program (<http://www.nsrl.nist.gov/votedata.html>). Has this been done?

A: They believed that this was being done and Sequoia would check on this and report back.

Q: Does this new version of WinEDS support the VVPAT add-on that will be used in NJ, or will further recertifications be necessary?

A: This WinEDS version does support the VVPAT add-on and should not need further changes, but the voting equipment itself (AVC Advantage and Edge machines) will require recertification both by Wyle labs and in NJ when the VVPATs are added.

Q: During the demonstration, one of the screens indicated that it is possible to “override the cartridge version check” via a single menu selection. Since the Sequoia representatives claimed that the cartridge version check is an important security control, why is it able to be disabled?

A: The Sequoia representatives were unable to answer this and said they would get back with information.

Q: During the demonstration, the operator password was viewable to everyone in the room (it was “password”) and appeared also to be changeable by the operator. Since this violates security protocols, why is this possible?

A: Ken Lanis explained that he was logged in with administrator privileges, and this would not happen for regular users. He suggested that the users should change their passwords when they get the system. (Note: it was unclear as to who would continue to have such administrator privileges when the software is delivered.)

Q: Since the connectivity to the Internet poses risks of contamination to the system that could potentially contaminate data, cartridges and equipment, potentially in future elections (as demonstrated in the Princeton experiments where a virus was transferred between voting equipment, even without Internet connectivity), why is this allowed, both by the State and the vendor?

A: The vendor claimed that Internet connectivity was an option that counties could choose to use or not. Richard Woodbridge claimed that it was out of the scope of the committee to make recommendations to the counties as to the use of the voting systems that they certify. Although the panel expressed that they do not feel it is appropriate to ever connect any part of the voting system to the Internet, or to use the report posting features that Sequoia provided in WinEDS, they did not believe that they could require that such facilities be turned off, nor could they issue advisories to the county election boards in this regard. The best they felt they could offer was outreach, such as this hearing being open to the county officials. Woodbridge believed that it was only the Attorney General’s office that could issue such advisories. (It was unclear as to whether or not the AG’s office would be doing this.)

Q: Sequoia claims that its ballot casting equipment (the Edge and AVC Advantage) is not vulnerable to the type of attacks demonstrated to be possible with some of the Diebold systems, yet the Sequoia systems have not been available for scrutiny sufficient to validate or invalidate these assertions. Given that Princeton University has successfully demonstrated the ability to easily contaminate and compromise a voting system using media that is akin to that in the Sequoia system, wouldn’t it be prudent to allow Ed Felten’s team to perform a similar type of experiment (under the auspices of non-disclosure agreements, as appropriate) on the Sequoia system in order to provide more confidence in these products, given that they are used by nearly all counties in the state?

A: Woodbridge felt that such testing would be unfair to Sequoia if it were not also applied to the other applicant systems. He explained that the state election codes were written in 1990, at the time lever machine technology was in place, and that it does not properly extend the panel's authority to institute such testing. His suggestion was that such investigation would need to be requested of and authorized by the Attorney General's office.

Questions from Lisa Gentile of Hudson County Board of Elections, and another person from Union County, pertained to the time it takes to perform ballot programming (currently in excess of 15 minutes per machine, longer if multiple languages are necessary), and the bugs experienced when moving layout files between WinEDS and Visio. Visio was briefly demonstrated with the new version and various warning messages first appeared on the screen -- ultimately it was shown to work only if the software security controls were reduced (from high to low), which was not questioned (with regard to security risks) by the examiners.

Some discussion also occurred during the Q&A regarding the production of training cartridges. The WinEDS system allows for the production of training cartridges that can be used multiple times without reprogramming. (Note: this poses a serious flaw that could enable vote erasure – it did occur when training cartridges were used in an actual election in PA, using the Danaher voting equipment. This possibility was not discussed by the examination panel.)

When Woodbridge asked the attendees for opinion or reaction to the new software, several election officials offered that they would like the update “yesterday,” seeming to press for this November's election, although it was not explicitly clear.

Irene Goldman expressed serious concerns about the features enabling Internet interaction, and suggested that these be required to be “turned off” (affirming the conclusions of the Red Team attack on the Diebold equipment) and added that “New Jersey should be a leader in this kind of security.” This was again referred to the Attorney General's office.

The Attorney General's office made inquiries regarding the types of statewide reports that would be available to them at the end of the election, using the new system. The Sequoia representatives said they would communicate further with them about that.

Various thanks were given by the Attorney General's office and the panel at the end of the session. Richard Woodbridge closed by saying “We haven't had Florida-type problems, and we are making sure that we have the right equipment so we won't.” It was suggested that any further remarks or questions from the audience should be sent in writing, quickly, to Maria Delvalle Koch of the NJ Division of Elections.

Some additional questions that came to mind following the session, that should be asked (in addition to a follow up request that should be issued for the answers to Rebecca Mercuri's questions that were not provided at the meeting, as noted above) include:

Q: Is this version of WinEDS being certified for immediate use (November 2006)?

Q: In reading the state laws (that were distributed at the meeting) it does not appear that the committee is limited in the scope of its investigation in terms of what was customarily done with lever equipment. In fact, when election laws were changed (some as late as last year), lever equipment was no longer being manufactured and was being phased out, so this assumption by the panel appears to be incorrect. Why isn't the panel performing the level of investigation necessary for the DRE systems?

Q: Why is the WinEDS software not considered to be part of the "voting machine"? How was this determination made?

Q: Given that the WinEDS software changes submitted for recertification directly affect the programming of the cartridges that determine the balloting and recording of votes, and given that the resulting cartridges control such things as the ability to vote for candidates (as per state law) as well as the ability to correctly record and accurately count votes (as per state law), it appears that the decision of the panel to waive the necessity of a "thorough" testing (as required by state law) via the recertification process was incorrectly made. How is it possible to justify this decision?

###