

Electronic Ballot Counting Device Advisory Committee
Meeting Minutes of October 12, 2009 at 9:30 AM
71 South Fruit Street, Concord, NH, HAVA Conference Room

Attendance:

Anthony Stevens, Assistant Secretary of State and Temporary Chair
Walter Fries, Moderator, Danville
Representative Richard Drisko
Representative Robert Perry
Stephen Edwards, Public Member
Adrienne Hutchison, Public Member

Secretary of State Staff:

David Scanlan, Deputy Secretary of State;
Daniel Cloutier, Assistant Secretary of State

Guests:

Jeff Silvestro, LHS
Gerry Bergeron, LHS

Also Present:

Melissa Bernardin

I. Call to Order

Anthony Stevens, Assistant Secretary of State, called the meeting to order at 9:38 AM. He stated Thomas Manning, Temporary Chair could not be here and he would chair the meeting in his absence. There was an official quorum. Mr. Stevens noted the last meeting's minutes would be taken up for approval later in the meeting due to a tight schedule constraint involving Jeff Silvestro and Gerry Bergeron from LHS who were due at 10 AM to provide answers to questions the committee had submitted to them.

II. Meeting Business

Mr. Stevens noted the constructive work done by the report drafting group, which includes Walter Fries and Representatives Perry and Drisko. Andrew Appel, Chair of the Computer Science Department at Princeton University, will be here for the meeting at the end of October.

Mr. Stevens discussed the text that the report drafting group had completed to date. The group had eliminated references to the "electronic ballot counting device", replacing it with "device". In the current version, "device" refers to the future and "machine" refers to the present.

Mr. Scanlan suggested that, in the "History" section, the following wording be replaced: "The Presidential Elections in certain other states in 2000 and 2004... and the general public." He thought it should read: "...by some election officials, activists and the general public". Mr. Scanlan suggested that it be noted where Harri Hursti's work was done - Leon County, Florida (greater Tallahassee). Mr. Scanlan said he has always acknowledged the Accuvote machines could be hacked by Harri Hursti. He pointed out that when he asked him to do it under election day circumstances, Mr. Hursti had declined.

Mr. Stevens said he had spoken with Mr. Hursti at the 2009 Usenix Conference. Mr. Hursti had said he needed time with the machine to effectively tamper with it.

Rep. Perry said the report language describes the conditions "under controlled conditions", but it deals with several significant possibilities. He pointed out that Diebold had stated the machine could not be hacked.

Ms. Hutchison said that the whole purpose of the paragraph was to acknowledge the hacking and that is one of the reasons we are here.

Mr. Fries noted the hack could take place while the machines are in storage and not necessarily on election day. Mr. Fries said the main thing was there had been a hack and it demonstrated vulnerability. It was enough to raise a question. Mr. Edwards asked to amend the paragraph to say; “not under election day conditions” instead of “under controlled conditions.” Mr. Scanlan asked how does it make it clear if it says “under controlled conditions”? Rep. Drisko wanted it to say “non-election day conditions.” Mr. Edwards said that was the point. Rep. Perry stated the hack could happen at any time, including during storage or transportation.

Mr. Stevens observed that it was 10 AM, the time when Gerry Bergeron and Jeff Silvestro were scheduled to discuss the questions posed recently to LHS by the Committee.

The following questions prepared by members of the committee appear in bold. LHS’s responses, emailed to the state, appear in red.

- 1. What will it cost to change out the current firmware in favor of the latest version that would-**
 - a. Handle NH’s ballot format**
 - b. Eliminate all or most of the identified deficiencies**

LHS answer: 239 machines need firmware only upgrade (to version 1.96.13 firmware)
@ \$75 installed.

Total = \$17,925

10 non lucid machines need readhead/firmware upgrade @ \$2495
installed.

Total= \$24,950

Subtotal= \$42,875

*If the firmware install is not done during periodic maintenance (PM),
then a \$100 service charge will be added per town.*

112 towns @ \$100

Total= \$11,200

Grand Total= \$54,075

Discussion:

Mr. Cloutier asked if it addressed all deficiencies, starting with the list identified by Voting Systems Technology Assessment Advisory Board (VSTAAB). (*Editor’s note: Working for the California Secretary of State and relying on researchers from University of California, Berkeley, VSTAAB had identified 16 vulnerabilities in 2006.*)

Mr. Silvestro said he thinks it eliminates all of them.

Mr. Silvestro answered that Nashua can’t use the GEMS software to consolidate ward results after an election. They will not be able to use GEMS for election programming; they must use multiple programs for the rotations.

Mr. Stevens stated he had the list of the 16 vulnerabilities found in the AV-OS.

(Editor's Note: The Department of State followed up on the 16 vulnerabilities identified by VSTAAB. ES&S/Premier provided a bullet list of fixes it had made to address each problem (see below). The test lab, iBeta, tested the system to the requirements of the VSS 2002. Brian Hancock, Director of Voting System Testing & Certification for the EAC, had advised the state in an email as follows: "The results of the California Top-To-Bottom Review as well as all other State test reports posted to the EAC Clearing House website as of 10 July 2009 were reviewed for impact to the test campaign." The California VSTAAB report does not appear on the EAC Clearinghouse site, but it is referenced in the California Top-to-Bottom Review that is linked to the EAC website.)

Attachment: ES&S reported changes to firmware version 1.94w, as reflected in firmware version 1.96.13.

California - Berkley Abasic Changes

Item	Description	What was done
V1	Array bounds violation	Added boundary check and return error if not valid
V2	Format string vulnerability	Do not pass string directly to format function.
V3	Input validation	Add validation
V4	Array bounds violation	Added boundary check and return error if not valid
V5	Double-free() vulnerability	Check for freed object before freeing.
V6	Array bounds violation	Added boundary check and return error if not valid
V7	Buffer overrun	Check requested size < available size.
V8	Buffer overrun, integer conversion	Check requested size < available size.
V9	Buffer underrun	Check index within range
V10	Buffer overrun	Validate parameters within ranges before use.
V11	Array bounds violation	Validate parameters within ranges before use.
V12	Array bounds violation	Validate parameters within ranges before use.
V13	Array bounds violation	Validate parameters within ranges before use.
V14	Pointer arithmetic error	Add check for end of data.
V15	Unchecked string operations	Validate parameters within ranges before use.
V16	Unchecked string operations	Validate parameters within ranges before use.

Follow-up committee question: Was it necessary to address these 16 vulnerabilities in order to achieve EAC 2002 certification?

LHS answer: Yes. The FEC 2002 Voting System Standard ("VSS") vol. II. 1.5 Evolution of Testing requires the VSTLs to conduct extensive tests on a voting system to evaluate it against new threats to a voting system as they are discovered, either during the system's operation or during the operation of other computer-based systems that use similar technologies to other voting systems. The VSTLs are required to expand their test to address the threats. Under the EAC Program, the VSTL is required to assess all reports listed on the EAC's website directory for Voting System Reports Clearinghouse and modify their test plans to include all applicable known threats.

As stated in iBeta Quality Assurance, Inc's Test Plan for the Assure 1.2 system, In accordance with VSS 2002 vol. II sect. 1.5, iBeta reviewed the body of knowledge deposited in the EAC's Voting System Reports clearinghouse for impact to the Security Test Method submitted herein. The results of the California Top-to-Bottom Review of the Premier system concluded that the vulnerabilities with the system depend almost entirely on the effectiveness of the election procedures. The VSS 2002 vol. I sect. 2.2.1 states that "System security is achieved through a combination of technical capabilities and sound administrative practices". This testing is conducted as part of the FCA Security Review and no additional testing was determined as a result of review. Review of the Kentucky, Ohio and Connecticut Reports resulted in no modifications to the Test Method as part of this Test Plan but did update the Security Test Case to verify that the Connecticut recommended tamper-resistant seals were incorporated into the Premier TDP. The review of the 3 March 2009 California Secretary of State report was also reviewed as well as the Premier Product Advisory Notices.

2. What is that version and which deficiencies will it and will it not address?

LHS answer: 1.96.13 AV-OS firmware
1.21.5 GEMS

- 1) From the literature provided by PES I see that GEMS 1.21.5 has blocked the use of MSAccess, improved database encryption/administrator password protection at sign in, and digitally signs the ABasic file. There is no central uploading or accumulation of results using GEMS in NH, so the upgrades to these features are not relevant.
- 2) The firmware 1.96.13 uses a Secure Hash Algorithm (SHA) to verify that the digital signature matches the digital signature stored on the .abo file. The firmware also checks counters for overflow, sum of all counters equals public counter and all candidate counters match the public counter. These checks are conducted at start up, memory card insertion, and when the ender card is inserted.

Discussion:

Mr. Silvestro stated that among Mr. Hursti's concerns was that the sum of all counters equals the total of all votes cast on the inside of the machine, a program that was inadequate to identify a certain type of tampering in firmware version 1.94w.

Mr. Cloutier noted that "Array Bounds" are 5 of the total 16 vulnerabilities identified by VSTAAB. LineV8 (*listed on the VSTAAB report*) states an "Array Bounds" situation could crash the machine. Since NH is a paper based state, a machine crash poses no fatal problem, Mr. Cloutier commented, since local election officials can hand count the paper ballots.

Mr. Fries wanted to know if there was a detailed response to all of the 16 issues. It would be very useful to have this for the record and to foster public confidence. Mr. Fries stated since LHS is the manufacturer's representative, it is important for them to have these responses, to know the story behind the list of vulnerabilities, and to ensure the manufacturer's responses are fully disclosed.

Mr. Silvestro believes there must be a 16 point response and said he will get it to the Committee. (*Editor's note: See above attachment, entitled "ES&S reported changes to firmware version 1.94w, as reflected in firmware version 1.96.13."*)

Mr. Stevens asked if there was a protocol available to check the encryption on the firmware chip of machines distributed in the field. This protocol would confirm that the software on the chip

approved in the test lab and certified by the EAC is the software that is being used on the Accuvote machine in the field.

Mr. Silvestro stated that the digital signature appears on the top of the printout.

Rep. Perry asked whether it is possible that the program could include the instruction to print that exact digital signature message, whether or not the firmware had been checked.

Mr. Cloutier asked whether the EAC certified the program that is on the chip.

(Editor's note: The EAC reports on its website that Premier Assure 1.2, which includes Accuvote firmware version 1.96.13 and the election management system GEMS 1.21.5, have been evaluated at iBeta Quality Assurance, an accredited voting system testing laboratory (VSTL), for conformance to the 2002 Voting System Standards and that this evaluation has been verified by the EAC in accordance with the provisions of the EAC Voting System Testing and Certification Program Manual.)

Mr. Silvestro stated that if one inserts a memory card, the AccuVote machine will reject the memory card if it does not match the chip.

Mr. Cloutier asked what comes out on the tape.

Mr. Silvestro stated the verification is performed on the report download. If the secure hash algorithm does not match the digital signature stored in the .abo file, "REPORT FAILURE" is displayed on the liquid crystal display (LCD) and "report verify failed" is printed on the tape.

Mr. Cloutier wanted to know if it can do an independent calculation. Is it set there as a number? He thinks it might be a program and can't compare two sets of numbers. A known hash number would be a way for a third party check. It should actually print out the hash, so one can physically read it.

Rep. Perry wanted to know what would happen if the memory card were swapped under these conditions. What hash would they have on there, real or compromised hash? Would the machine crash?

Mr. Silvestro stated the LCD would indicate "REPORT FAILURE" on the LCD display screen.

Mr. Fries wanted to know what sort of check occurs during the test in the two weeks prior to the election. Will the LCD indicate "REPORT FAILURE" if there has been inappropriate treatment of the machine chip or the memory card?

Mr. Cloutier thought this might happen if both the memory card and the chip were accessed.

Mr. Silvestro said that accessing the chip requires one to unscrew 5 screws on the machine.

Mr. Cloutier would like to see the discrepancy printed on the tape.

Mr. Cloutier stated tamper-evident seals go a long way; it would normally take more than one machine to alter election results.

Rep. Perry said we need to be additionally vigilant. Although these technicalities are over his head, he wanted to know how we get to the source and be assured these 16 deficiencies are fixed.

Mr. Silvestro believes there must be a list out there with a 16-point counterpoint with a certification from the manufacturer, Diebold/Premier, and some confirmation by the EAC that they have been dealt with. *(Editor's note: See above attachment.)*

Mr. Stevens said the National Institute of Standards and Technology (NIST) has an audit process to select Voting System Test Laboratories (VSTLs). By virtue of its signing an EAC certification document as a "VSTL", iBeta Quality Assurance was approved as a VSTL by the EAC as of the August 6, 2010 date of the certification signing.

Mr. Silvestro does not know if the 16 vulnerabilities had to be fixed in order to obtain EAC certification, but he understands they had to be addressed in the test process. *(Editor's note: See above attachment.)*

Mr. Cloutier stated that a hacker must be quite sophisticated to change both the memory card and the chip in the machine. The machine also must be available. He thinks tamper-evident seals might be the most effective method to deny hackers access and achieve security goals.

Mr. Bergeron said the seals only work if the seal protocols are strictly adhered to, and all changes are properly recorded. A post-election random audit is a good thing, he said.

Follow-up committee question: Is there a method of verifying the SHA (secure hash algorithm) by a 3rd party? If so, how?

LHS Answer: Since the SHA 1 has (sic) is part of the ABO file it is not possible to externally verify the SHA 1 has (sic) that is printed on the report. However the hash values of the certified reports is included in the information provided to the EAC and so the EAC can provide the hash values for the files and using those values toe riles can be externally verified.

Follow-up committee question: SHA 1/RSA verification: “If the hash does not match the digital signature stored in the .abo file, a “report failure” error is displayed on the LCD and “report verify failed” is printed on the tape.” If this occurs, is the machine still functional (can it accept ballots) or does the machine lock down automatically?

LHS Answer: The operator is informed of the error via the display and if they so desire they can proceed with processing ballots.

3. How long would it take (to install an upgraded firmware chip) assuming and following BLC approval?

LHS Answer: Approximately 2 months depending on the timing. If scheduled elections interfere with the installation, then the install would have to be delayed and may take longer.

Discussion:

Mr. Silvestro stated the two months depends on when the state’s Ballot Law Commission gives its approval. If they make a decision in April or May, it will be done by August. The normal NH maintenance period starts in January and lasts through April. If this approval goes forward, LHS will delay the maintenance and then do the upgrade and maintenance together. LHS will have its entire team work on the effort.

4. Does the 1.96.13 firmware chip currently exist, is there an available inventory of the product, and who is the manufacturer?

LHS answer: Yes it does exist, there is an inventory, and the chips are manufactured by Premier Elections Solutions, which was recently acquired by ES&S.

Discussion:

Mr. Silvestro stated the firmware version 1.94.w is the final version supported by VTS. As a result of the upgrade, he said, VTS (Voting Tally System, the legacy election programming software used with Accuvote) would be unusable. They would need to create multiple programs through the wards and could not use the GEMS software. Mr. Bergeron said that Manchester had opted not to use software to accumulate ward election results in the last election. Nashua used VTS to accumulate ward election results for both the 2008 primary and general elections. How much of an inconvenience would this be for the larger cities, he asked?

Mr. Cloutier asked whether the 1.96.13 firmware version and 1.21.5 GEMS would not have one database, but multiple databases.

Mr. Silvestro said any entity that opts to purchase GEMS for election results accumulation would be able to do so. This module costs between \$10,000 and \$13,000.

Mr. Silvestro stated Connecticut does not use GEMS for this purpose, because their regulations state that they are not allowed to use software for election results accumulation.

Mr. Bergeron said this software-assisted accumulation would be entirely for the press, to enable them to get the numbers and go home.

Mr. Stevens asked about the challenges associated with the software and columns on NH ballots. He wanted to know how the new software would satisfy NH needs and whether LHS can explain the related challenges.

Mr. Silvestro said the past version of GEMS had a five (5) column maximum, and every time you added a column you would have to readjust. He said that he got around it with GEMS. GEMS now allows the user to set up thirty-two (32) columns using intersecting points. The user can tell GEMS where to drop the ovals for the race. Columns can be the size the user wants them to be. This enhancement was made for landscape ballots, which CT uses. The user can set up intersecting points. GEMS allows the user to space the candidates.

Mr. Scanlan observed that the write-in column width had been necessarily a little narrower than the others in the past due to the shortage of space on the ballot.

Mr. Silvestro said he had tested the software.

Mr. Cloutier asked how long is the longest ballot - eighteen (18) inches?

Mr. Silvestro replied yes.

5. What will be the position of LHS regarding a decertification of the 1.94.w and the certification of the 1.96.13?

LHS answer: The State should be aware that this decision would cause VTS to be unusable. Without VTS Manchester and Nashua will be unable to electronically accumulate results on election night.

Discussion:

Mr. Silvestro said the existing Accuvote system will be supported as long as NH towns and cities wished to use it. There is really no clear answer regarding how it would meet future needs. If they were to create another version, they would then have to resubmit it to the EAC for a new EAC certification cycle.

Mr. Fries wanted to know whether there are any plans for updates in the near future.

Mr. Silvestro stated that if enhancements need to be made, they will be made and LHS will support NH equipment as long as needed.

Mr. Stevens asked whether ES&S is going to make that position official. He asked whether such ES&S position had been communicated to customers or just to LHS? Hopefully, the state can obtain something in writing, he said.

Mr. Silvestro said the main thing to remember is that the state's cities and towns are not going to lose any support.

Rep. Perry and Rep. Drisko said they remain skeptical due to the nature of the current transition.

Mr. Silvestro said he believes that, given the size of the Premier customer base that ES&S took on, ES&S would not risk alienating its Premier customers. There are voting machine companies such as Sequoia, Dominion and Hart who still have a substantial number of clients. Before the acquisition, Diebold/Premier had been the largest voting system manufacturer in the U.S., but the numbers would change if the comparison were made on a global basis.

Rep. Perry stated ES&S actually controls 75 percent of the machines (in the country) and the local vendors tend to be in control of the election programming. He wanted to modify his statement to read that 75 percent of the votes counted are through machines being supplied by one vendor.

(Editor's note: As of May, 2010, Dominion acquired rights to Premier Assure 1.2 (which includes firmware version 1.96.13 and GEMS 1.21.5) from ES&S under an anti-trust settlement with the U.S. Department of Justice. This transaction requires that current Premier customers be provided with the opportunity to assign their existing contracts to Dominion without penalty.)

Mr. Silvestro said that 75% of the machines are not being programmed by one vendor.

Mr. Bergeron pointed out that ES&S has not sold these Premier machines.

Mr. Stevens asked whether, as a result of the purchase, the LHS contract with Premier has been changed with ES&S. He inquired about the nature of the LHS contract with ES&S.

Mr. Silvestro said the dealership agreement involved all Premier products and the contract itself maintained they had to sell a certain percentage of New England's market share to carry it.

Mr. Stevens asked whether LHS has any pricing arrangements with ES&S.

Mr. Silvestro said LHS and other vendors would stay with the existing contract.

Mr. Stevens asked if there is any other ES&S vendor in New England.

Mr. Silvestro said no.

6. Is the 1.96.13 just the latest firmware version or is it the end of the line for Accuvote firmware versions?

LHS answer: It is unclear if this will be the last version of AccuVote firmware.

Discussion:

This matter was covered in responses to the previous questions.

**7. Can the 1.96.13 itself be modified or would future changes require a new chip?
a. If the answer is, yes, it can be modified, what security issues does that raise?**

LHS answer: No. Future firmware upgrades would require installation of a new chip.

Discussion:

Mr. Silvestro said that the 1.96.13 chip can't be modified. It needs to be removed and a new chip inserted.

Rep. Perry said he wanted to know if the chip could be reprogrammed not in, but out of the machine. Mr. Silvestro said he had just answered that. The answer is no.

8. What, if any, issues are created by removal/deactivation of the serial port on the Accuvote?

LHS answer: LHS would suggest disconnecting the wire from the mother board and then cutting the wire harness thus leaving the RS232 port and eliminating the creation of a hole. The serial port pins could then be damaged, further rendering the port visibly disabled. This operation would be performed by our technician and witnessed by the clerk. Both parties would then sign a document attesting that the operation was completed. The document

would then be submitted to the State as verification that the serial port has been disabled. This would be the most cost effective and technically functional option.

- a. If the serial port were physically removed from the back of the machine leaving an open hole, can that hole be covered with a plate?**

LHS answer: Yes, this is an option. However it should be noted that disabling the serial port will render the machines unable to communicate with GEMS.

- b. What would be the cost associated with this?**

LHS answer: Who would be responsible for creation of a plate cover for the hole? Would this operation occur during PM's (periodic maintenance) or would it be done separately? Cost to be determined later. My answer to question 8 is a cost effective solution.

Discussion:

Mr. Silvestro said if you are considering doing this removal and deactivation of the port, he would suggest disconnecting the ribbon cable from the mother board and cutting it at the harness. The state would create a form describing the procedure and have it signed by the clerk and the LHS machine technician. This will disconnect the serial port. It will not leave a hole in the back of the machine and no one would be responsible for providing a plate to cover this hole. It is cost effective and is the best way to proceed.

Rep. Perry and Mr. Cloutier asked about cutting the wire and pins, and crimping to distort the serial port, so that the general public can see it has been distorted.

Mr. Silvestro said distorting the serial port would be easier.

Mr. Stevens inquired whether this is part of the \$17,927 charge quoted.

Mr. Silvestro stated if this procedure were done during the preventative maintenance, there would be no additional charge.

Mr. Cloutier suggested the process should result in the visible appearance that no one could even plug into this physically distorted port.

Mr. Silvestro said that whatever NH needs to get done, it will be done. If NH needs a document, this would be fine with them and it would be signed by everyone. The whole state could be finished in two months.

Mr. Cloutier asked whether LHS could distort the telephone port as well.

Mr. Bergeron said they could have a plug-in glued into the port, one which cannot be pulled out.

Mr. Silvestro stated that not all AccuVote machines in NH have modem ports. With this procedure, the state would effectively eliminate any chance to use VTS. LHS has four (4) people on the maintenance staff and together they pay a maintenance visit on each machine once a year.

Mr. Stevens stated the clerks would need to be prepared for this process.

Mr. Silvestro said most clerks stand there and watch during the entire maintenance call. Most locations have only one machine, so it will not take long. The Secretary of State would need to explain to the clerks how to disable this port.

- 9. Is there any means by which the machine firmware, memory card or other feature can be disabled or altered by remote means?**

LHS answer: No.

a. If yes, is shielding a fix?

Discussion:

Mr. Silvestro said No; if any modems in a machine have been turned off, they all have been turned off.

Mr. Cloutier said the modem could be removed and the serial port disabled. There are no wireless capabilities.

Rep. Perry asked what would happen if someone strolled by with a powerful magnet.

Mr. Bergeron said a magnet would not change anything on the ballots, which could be counted by hand if the machine failed.

Mr. Fries asked if the machine modem has necessary access to be functional. If he carried in a wireless modem, could he access the machine modem?

Mr. Bergeron said that since 1994, the only way to communicate with the AccuVote machine is through a telephone upload to a central computer.

Ms. Hutchison asked whether there is a USB port on the AccuVote machine.

Mr. Cloutier said no.

Mr. Silvestro pointed out that this is 1992 technology.

(Editor's note: Subsequent discussions with LHS and ES&S reveal that the Accuvote machine passed the environmental tests by SysTest Labs (an Independent Testing Lab under the NASED program) required under the 2002 NASED/FEC Voting System Standards (2002 VSS). When the EAC and the National Institute of Standards and Technology (NIST) established testing protocols for the 2002 VSS, they initially relied on the original environmental testing that had been conducted by Sys Test Labs. Later, when NIST had established and qualified Voting System Test Laboratories (VSTLs) under a new regime, they elected to require new tests under new protocols. These protocols called for 8,000 volts to be applied to numerous physical locations on the machine during counting. While similar testing had occurred under Sys Test Labs, iBeta, a NIST-qualified VSTL, found a vulnerability involving one location on the machine that locked up the machine but did not affect the counting mechanism. The machine had to be rebooted and re-started; hence, the vulnerability was not considered critical. The Assure 1.2 hardware EAC certification for the Accuvote machine requires a \$300-350 installation of electrostatic shields. Although 6 states have recently purchased the 1.96.13 upgrade, few, if any, require these shields. The reason is that there is a simple work-around in the unlikely event that 8,000 volts is applied to that one location on the machine: restart the machine and run the ballots through the machine again. The New Hampshire Ballot Law Commission's Order #BLC 2010-3 dated April 20, 2010, which approved the firmware version 1.96.13, did not require this change to the equipment.)

10. What is the function of the clock chip?

LHS answer: The clock chip is used to time stamp reports that are printed on the AV-OS and to time stamp audit log on the memory card.

a. How would (the clock chip's) removal affect the operation of the machine?

LHS answer: None.

b. Were the concerns over the presence of the clock chip permitting a timed attack justified?

LHS answer: I am not aware of any simulation or attack like this ever happening. If it is a concern, the clock chips can be set to the time and date of the election during the pre election test.

c. What would be the cost associated with removing the clock chip?

LHS answer: If this procedure occurred during PM's (periodic maintenance) there would be no cost associated with the operation.

Discussion:

Mr. Silvestro said the time stamp inputs to an audit log. If you remove it, no stamp will be on the reports. The clock chip is as accurate as the programmer.

Mr. Cloutier thought it may not be using the mother board battery. Could it be drawing from an internal battery in the clock chip itself?

Mr. Bergeron said one must replace the clock chip itself to replace the battery.

Mr. Stevens said that the state finds the clock time-date marks on the election results tape useful when they analyze the tapes.

Mr. Bergeron said it is up to the user to keep the clock chip set appropriately. It is fairly easy to set and it does not lose time when set 10 days prior to an election.

Mr. Stevens said it was used for when the state or local election officials review the tape.

However, some are worried about outside sources being able to access it.

Mr. Silvestro said there are instructions for people to follow, a counter setting test with the election date.

Mr. Stevens asked if there was any way one could connect the clock chip with the machine chip.

Mr. Silvestro stated he has not ever seen anything else it could be utilized for, other than election results reports and audit reports.

Mr. Cloutier said he felt there may be little to gain by removing the clock chip.

Mr. Fries asked if it strictly provided a time-date stamp on the tape report.

Mr. Silvestro said yes.

Ms. Hutchison asked if you could run tapes during the day.

Mr. Silvestro said if you wanted to print an audit log, you would not be able to do so if the clock chip were gone.

Rep. Perry said there had been a problem in Rochester. The machine tape did not reflect a vote tally until 8:20 AM, 20 minutes after the polls opened. He wondered if it could have been a problem with the clock chip.

Mr. Silvestro said it sounded like a bad memory card.

Mr. Stevens asked if it could be a bad battery or a clock that had fallen behind and had not been updated by the election official during pre-election testing.

Mr. Bergeron stated he did not know how this could happen. If the card is corrupted, it will not accept the ballot.

Mr. Silvestro noted there had been a ballot problem in Massachusetts. It could have been a case of bad ballots.

Mr. Bergeron said the election official would have noticed that.

Rep. Perry said he recently went to observe a machine on election day. Voters would put their ballots in the machine, which rejected the ballots and pushed them out the direction they had been inserted. In some cases, voters had to be called back to re-insert their ballots.

Mr. Fries stated he thought, at times, 20 percent of the ballots do get kicked back in his town, particularly when they are not fed in straight or they are pushed in by the voter (not pulled in by the machine). The machine only reads these ballots the second time after they are submitted more carefully.

Rep. Perry asked if the clock chip had been removed by any other jurisdiction.

Mr. Silvestro said a couple of Massachusetts towns have not replaced worn-out clock chips, because of the cost. They cost \$35.00 apiece. He stated if the removal of the clock chip was done with preventative maintenance, there will be no cost. As to the timing of the maintenance visits in 2010, he will have his people start in Vermont and delay NH preventive maintenance. He will ask his maintenance department what the drop-dead deadline would be. He understands that timing is crucial to make the machines usable in the September Primary. Given this plan, maintenance would probably be finished by the end of June or early July.

Mr. Stevens asked if the seal format specs have changed.

Mr. Silvestro said he really likes the wire seals with the twists. They do not break as easy as the plastic. The wire seals with the twists stand up and are more sturdy. The same seals are used in the medical fields. If the wire is not put on properly, it is harder to close the ballot box. He suggests staying with the current tamper-evident wire seals.

Mr. Bergeron wanted to talk about the older read non-lucid read heads, the ones that need to use the marking pens (that may not work with some ball point pens). There are 10 such machines in the following 6 towns:

- Somersworth – 5 wards
- Canterbury
- Gorham
- Littleton
- Loudon
- Pembroke

(Editor's note: According to LHS, all of the above communities obtained lucid read heads in 2010.)

Mr. Bergeron has a list of 6 school districts which operate a total of 8 AccuVote machines in school elections. Any changes required for the town and city machines should be applied to the school-owned machines. The 239 machines listed in the state include 8 SAU-owned machines.

Those SAU's are:

- SAU 72 – Alton
- SAU 19 – Goffstown
- SAU 24 – Weare
- SAU 28 – Windham and Pelham (one machine each)
- Oyster River – Durham
- Governor Wentworth (two machines)

(According to Mr. Silvestro, all of the above school machines have lucid read heads.)

Mr. Cloutier asked what if one machine is programmed to receive two ballots.

Mr. Silvestro said the issue would need to be addressed and it would cause confusion.

Mr. Stevens asked if you could set the machine to reject only blank-voted ballots (ballots on which the machine could find and read no marks in the ovals).

Mr. Cloutier clarified by presenting the following scenario: if someone wishes to cast a ballot but does not want to cast a vote for any candidate and makes no marks on the ballot. How does the voter get the machine to count the ballot?

Mr. Bergeron said it would require a manual over ride on the front of the machine to force the ballot into the machine.

Mr. Cloutier suggested that someone might learn the voter is casting a blank ballot. It can be a privacy concern.

Mr. Bergeron said in other states it was not a problem that has been documented.

Mr. Silvestro said they were not allowed to program the machines to reject (undervoted or overvoted) ballots in NH.

Mr. Stevens said the Committee needs to think about the 6 towns/cities with non-lucid read heads. It would cost \$2,495 per machine to change the read heads.

Mr. Silvestro explained that LHS has not tested the new chip (version 1.96.13) with the existing Accuvote machine. LHS has tried to use the newer chip in those machines. If it is your goal to have standards, they need to be updated to cover those old read heads. *(See editor's note above.)*

Mr. Stevens asked whether LHS thought the wire seals are adequate.

Mr. Silvestro said yes, they are, but they are only considered tamper-evident. If you take it another step and use locks, then you would need keys.

Mr. Stevens stated that careful recording of seals has to be performed by election officials and the clerks and moderators need to receive continued training with the seals and machines.

Mr. Cloutier said the moderators need to be instructed to look at the seals.

Mr. Silvestro suggested post-election random audits are a good idea.

Mr. Fries said that, in the past, few people have paid attention to the number on the seal. Mr. Stevens said it is possible that inspectors from the Attorney General's office can be instructed to look for the procedure in subsequent elections, although they may need a law or Ballot Law Commission ruling to do this. *(Editor's note: The seal for ballot containers now pointedly asks for the number of cast ballots in each ballot container. The 2010-2011 Election Procedure Manual now has an example of a properly completed seal.)*

Mr. Fries said you need someone to deliver the seal numbers and it needs to be recorded in some independent place.

Rep. Perry asked whether either Mr. Silvestro or Mr. Bergeron know who owns ES&S?

Mr. Silvestro stated he believes there are actually three parties who own it and he wanted to get back to the board to get it straight.

Rep. Perry read from an attachment to a September 25, 2009 letter from Black Box Voting to the Anti-Trust Division of the U.S. Department of Justice. The attachment, which partially describes ES&S ownership, appears below:

APPENDIX A: PARTIAL UNRAVELING OF OWNERSHIP TRAIL ON ES&S

ES&S is privately owned; the names of its current owners have not been publicly released, but articles in the Omaha World Herald indicate that:

- ES&S is or has recently been owned by The McCarthy Group and the Omaha World Herald and/or The World Companies (also affiliated with the Omaha World Herald Companies). The Omaha World Herald is a media conglomerate; this ownership links control of media outlets with control of programming for devices that elect federal candidates.
- The McCarthy Group, in turn, is or was partially owned itself by the Omaha World Herald and/or the World Companies.

The Omaha World Herald and the World Companies have been owned by the Peter Kiewit family, owners of privately held Peter Kiewit & Sons, a privately held diversified multinational company handling road construction, communications, and the building of defense installations. The Omaha World Herald became an employee owned company shortly after Peter Kiewit's death, but with restrictions on employee stockholder voting rights. According to the Omaha World Herald, the Peter Kiewit Foundation holds the largest shares in and the most voting rights for the Omaha World Herald Companies.

Mike McCarthy, who runs The McCarthy Group, handled the sale of Peter Kiewit's ranch when Peter Kiewit died; just after Peter Kiewit's death, McCarthy capitalized and launched The McCarthy Group. Mike McCarthy is a board member for Peter Kiewit & Sons; Mike McCarthy's family relationship within the Kiewit family, if any, has not been publicly disclosed. In examining the impact of this acquisition, the relationship of ES&S owners to members of the Kiewit family or to the Kiewit organization or companies should be more fully explored, because Kiewit companies and key personnel were repeatedly convicted of unfair trade practices and bid-rigging several times in the 1980s, and of various unfair trade practices in the 1990s. The Kiewit company paid several fines for setting up companies posing as unrelated to Kiewit, which were in fact owned by and/or controlled by Kiewit personnel, and some key executives were sentenced to prison.

ES&S reported on public bid forms submitted to Santa Clara County, Calif. in 2003 that another group of investors called "Normal Investments LLC" owns part of ES&S. The names of the investors in "Normal Investments LLC" has not been publicly disclosed.

An Omaha World Herald article also indicated that a group of investors composed private investors associated with the original Business Records Corporation entity owns part of ES&S. Their names, and what percentage they own, has not been publicly disclosed.

Without knowing the names of investors in ES&S, it will not be possible to examine this acquisition for past history of unfair competitive practices by its owners. An organizational review needs to be part of investigation into this acquisition. It should be noted that majority ownership does not settle the finite question control of all or part of the company. For example, not only may minority shareholders negotiate or retain special rights upon sale of a majority share of stock, but even an employment contract could reserve powerful rights to some person or persons to access or control software.

Rep. Perry stated in summation he was personally very concerned regarding the purchase of Diebold by ES&S.

Mr. Silvestro said he would like to get the actual names before he commented.

Rep. Drisko observed that Kiewit, one of the reported owners, was roughly on a par with Perini Construction and had international operations.

Mr. Silvestro said he would like to know if, in fact, these companies have an actual say in the control of the company. He has personally met Matthew Nelson, ES&S's Senior Vice President of Sales. He reiterated it is business as usual with them at LHS.

Rep. Drisko stated there is a great concern, as they are not a parent of LHS, but LHS is its own parent company.

Mr. Silvestro stated that LHS is its own entity and has its own thought processes.

Rep. Drisko said that the control aspect of LHS's supplier is a concern. The playing field could change due to their view of LHS's track record in the field. He stated that it is a concern for (LHS and NH) and he does not see another alternative.

Mr. Silvestro said you could go to Hart, Sequoia or Dominion and get quotes and start over.

Mr. Bergeron said LHS has ample amount of spare parts available for the Accuvote line in New England and still does repairs on the older Optech machines. We take care of our customers, he said. Mr. Silvestro added that at this time they would be able to do 20 years of maintenance on the Accuvote machines.

Mr. Edwards said the procurement is critical and addressing integrity and capability. The responsibility of confidence is distributed by its jurisdiction and boundaries.

Rep. Perry talked about the public's perception. His concern was for the upcoming election. All these vendors have proprietary claims on all these machines and software, he said.

Mr. Silvestro stated that Connecticut owns a license for GEMS. Many of the reports issued by CT support the machines.

Mr. Stevens said he had asked Connecticut's Deputy Secretary of State if they would give NH full access to the source code-related work of UConn's Voting Technology Research Center. She said no. Without a waiver from Premier, the CT Secretary of State could not provide the source code to NH. Mr. Stevens asked if there were a written protocol to obtain access to all of UConn's work and analysis.

Mr. Silvestro said no. His impression was that states could request to review it, but the release of details may be limited.

Mr. Edwards asked whether the state could seek to amend the contract and specify this component to the contract.

Mr. Edwards observed that the state holds tremendous power in this situation.

Mr. Fries noted that his experience is that companies will disclose this kind of information under controlled circumstances.

Mr. Cloutier said GEMS software is irrelevant and we want to see the software written on the firmware version 1.96.13. How does it tabulate?

Rep. Perry stated Harri Hursti suggested that a Cropscan unit can be used to read an obsolete memory card, but as a practical matter an updated Cropscan unit does not exist.

Mr. Cloutier stated that the Cropscan unit actually reads the Accuvote memory card but it takes too long (about 56 minutes) to read it to render it useful in a thorough review of memory cards. Harri Hursti could probably get it down to 4 minutes (per card).

Mr. Silvestro said UConn had accomplished a shorter read time with their software. Mr. Cloutier said it was the quick read software they were not willing/able to share.

Mr. Stevens said the UConn Voting Technology Research Center has done a lot of analysis on Accuvote optical scanning machines. NH might be interested in their work to reverse engineer the software code. NH, along with the general public, already has access to UConn's reports, which appear on the EAC website at

http://www.eac.gov/testing_and_certification/voting_system_reports.aspx

NH does not have \$250,000 a year, roughly the amount the Connecticut Secretary of State pays UConn, to fund a similar effort.

Mr. Cloutier asked why the committee needs to see GEMS.

Mr. Silvestro said GEMS source code is not what you are looking for.

Mr. Cloutier said he is interested in the source code that is on the chip that is in the machine, and that writes the code.

Follow-up committee question: Who owns ES&S? Who makes up the Board of Directors?

LHS Answer: Please refer to the Manufacturer's Registration available on the EAC's website for ownership and board of director information for both the ES&S and PES organizations.

http://www.eac.gov/index_html/program-areas/voting-systems/docs/es-s-manuf-reg-revision-letter-10_1_09/attachment_download/file

http://www.eac.gov/index_html/program-areas/voting-systems/docs/pes-manuf-reg-revision-letter-10_1_09/attachment_download/file

Follow-up committee question: Is there a quick-read version of the 1.96.13 code and memory card layout available to the state for review?

LHS answer: I do not know what a 'quick read version' of the code is. Yes the memory card layout is available for state review. Please note that that information is proprietary and not to be disclosed to others without ES&S's written consent.

Follow-up committee question: Is the 1.96.13 full code available for review?

LHS answer: All source code was reviewed by an accredited VSTL and determined compliant to the VSS standard by the EAC. Source code is proprietary and not generally available for outside review without strict non-disclosure agreements between ES&S and the reviewer. ES&S is willing to further discuss the release of the requested firmware if desired.

Mr. Silvestro stated he wanted to review the committee's follow-up question. He was going to get back to the committee with further answers. (*Editor's note: See follow-up committee questions and LHS answers included above.*)

Mr. Silvestro and Mr. Bergeron left the meeting at 12:25 PM.

The committee recessed for lunch at 12:25 PM for a half hour.

The committee resumed the meeting at 12:56 PM.

III. Meeting Minutes

Mr. Stevens asked the committee to review the July 27th Meeting Minutes.

Mr. Fries pointed out the term "single step approach" on page 3, 3rd paragraph from the bottom. Mr. Fries thought the term could be misinterpreted to mean sole source bids. Mr. Stevens agreed to omit "single step approach" in the sentence.

Mr. Fries questioned why VVSG 1.1 would be referenced as a source document in the RFI. Mr. Stevens explained NIST (National Institute of Standards and Technology) created the set of somewhat detailed requirements. The large document is something vendors recognize.

Mr. Stevens asked for a motion to accept the July 27th, 2009 meeting minutes. Ms. Hutchison and Rep. Perry abstained from the acceptance of the meeting minutes, as they were not present at that meeting. Mr. Fries made a motion to accept the meeting minutes and Rep. Drisko seconded the motion. All were in favor, and the motion passed.

Mr. Stevens asked the committee to review the September 14th meeting minutes.

Ms. Hutchison asked if Senators Shaheen and Gregg had responded to the Clerks' petition regarding Senator Schumer's bill (the MOVE Act). Mr. Stevens said Senator Gregg had sought a carve-out for states like New Hampshire based on good performance in counting UOCAVA absentee ballots. Senator Shaheen's office said they would contact the clerks who signed the petition directly.

Mr. Fries commented on page 1, paragraph 4. He wanted to have the following phrase inserted in the last sentence: "under which the state requires that all towns and cities be placed on a "most favored customer" list, so that all towns and cities get the (insert "best" – omit "same" price and conditions protections) that the manufacturer/dealer offers to anyone.

Mr. Edwards wanted to know about specific options for New Hampshire and where significant savings opportunities in machine software and hardware acquisition might be achieved.

Mr. Stevens explained that customarily one state on the "bleeding edge" ventures out and tries out a new software and hardware package created by a vendor. After they have expended considerable effort and fully adopted the software and hardware, other states learn from this state and may decide to follow and customize the application to their state. Because of marked differences among the states, it normally takes a period of time, sometimes years, before a product is truly past the beta stage and can be sold to a number of states without significant changes and improvements. There is a relatively high cost of development, partly because of differing laws and protocols among jurisdictions, as well as certification. This principle would still apply if a new more ideal system were developed; it might take years before it was ready to be sold in large quantities in many states. Even then, the state and local jurisdictions' major savings opportunities would probably lie in hardware and software design, and operating costs such as election programming, ballot printing, ballot on demand and reduction of ballot proofing at the data interfaces. He felt that the savings achievable through volume acquisitions of hardware, although significant, would be minor by comparison.

Ms. Hutchison said due to her medical treatment on October 22nd, she would not know if she could attend the next meeting on October 30. She needed to leave the meeting for a 2 PM appointment. Mr. Edwards and Rep. Perry stated they were planning to attend the October 30 meeting. Mr. Stevens stated they needed to review the dates to get the final report in a final form. Mr. Fries said he would be gone for the last two weeks of October.

Mr. Fries noted the typo on the page 6, the last page. The next gathering of the Report Subcommittee should read October 13 rather than October 18 and the time should read 1PM, not 1:30 PM.

Rep. Drisko moved to accept the September 14th, 2009 meeting minutes. Rep. Perry seconded the motion. All were in favor and the motion passed.

IV. Meeting Business

Mr. Stevens asked the Committee to address the final report draft. Mr. Stevens wanted to advance the requirements a step further based on the morning's discussion with LHS regarding the upgrades available.

Rep. Perry and Mr. Fries agreed that removing the clock chip might not result in a net improvement.

An Accuvote machine was brought into the room for the Committee to enable an inspection of the position and function of the wire and tape seals. Mr. Stevens explained there is no existing law that enables the Department of State to establish requirements for the seals. (*Editor's note: RSA 656:42, as revised in 2010, now contains seal requirements.*) After some testing, Mr. Fries wanted the Committee to ask LHS to ensure the seals are more tamper proof than the ones he saw demonstrated. By using twisting wire seals instead of plastic seals and by tightening up the twisting wire seals to eliminate any excess wire, certain observed vulnerabilities can be eliminated.

Mr. Edwards explained that his business sells to the auto industry. VIN numbers are all over a car. If you take them off, the fluorescent number remains and it is obvious that the vehicle has been tampered with. Tape seals have a wide range of capabilities and costs. All agreed the state should approach LHS to further research seals.

The committee recognized that if the state must use an Accuvote machine, it must be updated to 2002 Voting System Standards. Mr. Fries wanted it on record that he thought LHS should be liable for the upgrade. He said the defects are clearly defects that can be corrected. The necessary upgrades could be reasonably scheduled as part of annual preventative maintenance and LHS ought to be told that.

Rep. Drisko excused himself from the meeting at 3:22 PM. Mr. Edwards left shortly after Rep. Drisko.

A discussion followed pertaining to on-site audits after the closing of the polls. There was no quorum present at this time.

The meeting was adjourned by Mr. Stevens at 4:20 PM.

Minutes taken and typed by: Colleen McCormack-Lane

Adopted by Committee:



Anthony Stevens, Temporary Committee Chair

Date: December 17, 2010