2007-01244

September 28, 2007

The Honorable Greg Stumbo
Attorney General
Commonwealth of Kentucky
700 Capitol Ave., Ste. 118
Frankfort, KY 40601

Re: *Improving Kentucky's Electronic Voting System Certifications*

Dear General Stumbo,

Thank you for the opportunity to join your staff at the State Board of Elections recertification on September 17, when the SBE reviewed the ES&S, Hart, and Diebold[1] systems.

I have divided this report into two major sections: observations from the recertification meeting and recommendations for the future.

Observations

My observations from the recertification meeting are as follows. I have divided these into general observations and those specific to each of the three vendors.

General: All three vendors came in prepared to demonstrate their products. The purpose in their mind did not seem to include an in-depth look at possible issues with the machines. Among my observations of the review process:

- The certification does not include the ballot programming and tallying components (such as Diebold GEMS or Hart BOSS). As pointed out by the California study[2], the central server is one of the weak points in the voting system, especially with respect to introduction and spread of malicious software, this is a critical omission.
- While each of the vendors demonstrated their systems with the optional paper trail modules, it was unclear whether the paper trails are in fact in use in all Kentucky counties. If they are not, it is questionable whether the certification would apply to those counties.
- The review relies on the completeness and accuracy of the testing by the Independent Testing Authorities (ITA) for conformance to the voluntary Federal guidelines (Voting

[1] Diebold Election Systems Inc (DESI) has renamed themselves as Premier Election Solutions. They are a wholly owned subsidiary of Diebold, Inc. Throughout this report, the company is referred to as Diebold, for consistency with the outside studies.

[2] Redacted versions are available from the California Secretary of State web site at http://www.sos.ca.gov/elections/elections_vsr.htm.

Systems Standards 2002[3]). However, it has been well established that the ITAs do not adequately perform this role. For example, Ciber (the primary ITA used for software testing) was suspended from its testing role by the US National Institute of Standards and Technology (NIST) due to its inability to show that it actually performed the required tests[4]. As noted by Professor Michael Shamos[5], a long-time defender of DREs:

- *Too many systems pass ITA qualification but shouldn't*
- *State certifications can't replace ITAs – too brief, too cheap*
- *Required pre- and post-election testing is often not performed*
- *Acceptance testing is not revealing unreliable machines*

- The ITA reports[6] used for Federal certification and included in the review packages used by the SBE certifiers are cursory.
  - Source code: The source code reviews are focused on the *syntax* of the source code, noting facts such as where headers or comments are missing and software modules longer than the recommendations[7], and not on the *semantics* of the code where security flaws would be found. This is reinforced by the fact that none of the ITAs identified the flaws found by the California or Florida[8] source code review teams.

[3] No longer available on the US Election Assistance Administration (EAC) web site, but available from http://www.verifiedvotingfoundation.org/downloads/fecvss20020430.pdf

[4] The letter terminating test lab accreditation can be found at http://www.eac.gov/News/press/docs/06-13-07-commission-votes-to-terminate-ciber-interim-accreditation-application. Additional information about Ciber's test lab accreditation can be found at http://www.eac.gov/voting%20systems/test-lab-accreditation/interim-accreditation/pending-applications.

[5] Excerpted from *Security, Paper Trails, Accountability*, slide 3, presentation by Michael Shamos, Voting Systems Testing Summit, Nov 29 2005. Professor Shamos has been responsible for over 100 Pennsylvania voting machine certifications from 1980 - 2000 and 2004 to present. He notes that "over 50% of systems fail state certification, about 25% for reasons particular to Pennsylvania". By contrast, according to www.elect.ky.gov/votingsystems.htm, it does not appear that Kentucky has failed any machines for state certification in at least ten years.

[6] These reports contain proprietary information of each of the three vendors, and hence are not described in detail.

[7] These flaws are indications of poor software development practices, but are not *a priori* software flaws. They are akin to inspecting the paint on a new car as an indicator of the reliability of the vehicle. While a poor paint job may be indicative of sloppy manufacturing, a good paint job is not necessarily indicative of a reliable vehicle.

[8] Redacted versions are available from the Florida Department of State web site at http://election.dos.state.fl.us/pdf/SAITreport.pdf. A supplemental report is available at http://election.dos.state.fl.us/pdf/DieboldSupplementalReportFinalSubmission.pdf.

  - Testing: The testing is limited to *functional* testing, namely a verification that the systems do what they should in normal circumstances. There is no indication of any *stress testing* where the system is tested in unusual circumstances, or *security testing* where the system is tested to determine that it does not do anything it should not do.

- Because the ITA reports are of limited value, the quality examination of the machines as part of the certification processes is crucial, but it too can best be described as cursory. There was little effort to test the limits of the machines, including:

  - In no case were more than a handful of votes cast on any single machine (either optical scan or DRE). As there have been problems reported in the past with voting machines unable to handle a reasonable number of votes[9], this would be a worthwhile test.

  - For the two vendors with touchscreens (ES&S and Diebold) there was no effort made to see the results of common voter errors, such as dragging a sleeve across the screen or dragging a finger across the screen while depressing a candidate's name.

  - For the two vendors with touchscreens, there was minimal discussion and no demonstration of the screen calibration[10], and when it should be performed.

  - Where write-ins were attempted, there was no effort to see what would happen if the voter typed an overly long or deliberately malformed name[11].

  - For those machines with paper trails, there was no discussion of handicapped accessibility to the paper trail.

  - There was no discussion or examination of the physical accessibility aspects of any of the machines. As noted in the California accessibility report[12], this is a major problem with all of the voting systems.

[9] For example, a recent North Carolina election where the DRE could only accept 5000 votes. One of the machines was used for early voting by approximately 7500 voters; the votes of the last 2500 were lost. Whether an error was given by the machine prior to allowing the lost votes is a matter of dispute.

[10] Calibration refers to setting the machine so that a touch on the screen causes a selection to be made for the proper candidate, and not for an adjacent candidate. Problems with calibration are one cause of "vote flipping" where a voter attempts to select one candidate and actually selects an opposing candidate.

[11] A common cause of security problems on web sites is where users deliberately type input that causes the underlying databases to perform unplanned activities. This might be possible with DREs or ballot marking devices, depending on their implementation.

[12] Available from the California Secretary of State web site at http://www.sos.ca.gov/elections/voting_systems/ttbr/accessibility_review_report_california_ttb_absolute_final_version16.pdf

- The physical keys used to protect the restricted portions of the machines (such as printers and ballot storage bins) appeared to be of a low quality[13]. None of the examiners asked whether the keys are the same on all machines made by that vendor for use in Kentucky, or for that matter anywhere else in the world. If the keys are not relatively unique, they are generally worthless, and the use of numbered seals and tamper evident tape must be considered as the only physical security measure that protects the machines from tampering.

- With the exception of the ES&S AutoMark, all of the printers used thermal paper, which has a fairly short lifetime before the print begins to fade[14]. Kentucky law only requires keeping paper for 60 days[15], but Federal law appears to require 22 months in some cases. There was no discussion about the proper environmental conditions as to ensure the paper meets those requirements.

- There was no discussion of the privacy and anonymity implications of recording votes on a continuous roll of paper[16].

- There was no discussion of machine reliability, which has been a major concern in many states. The Federal voluntary standards allow for a high failure rate which must be taken into account in determining the appropriate number of machines to acquire and place in polling places.

- There was minimal discussion of multi-lingual ballots, and measures to ensure that votes are counted correctly in all languages. If Kentucky is a state which has obligations to provide ballots in multiple languages, this is important to test[17].

- There was no discussion of whether particular types of pens or markers are required for optical scan ballots for each vendor's equipment, and if so what the results would be of using other types of markers.

[13] A recent Princeton study showed the risks of poor quality keys in voting systems. See *Security Analysis of the Diebold AccuVote-TS Voting Machine,* Ariel Feldman, Alex Halderman, and Edward Felten, http://itpolicy.princeton.edu/voting/.

[14] The lifetime depends on the conditions in which the paper is stored; in particular, heat tends to cause faster fading.

[15] As required by KRS 117.275(8).

[16] If a record is kept of the order in which voters cast their ballots, or the time at which voters enter the polls, this can be used to match votes to voters, violating privacy. Additionally, use of a single voting machine in a precinct dramatically increases the risk of privacy violations under these conditions. Whether this is a meaningful may depend on individual county policies for keeping voter records, as there do not appear to be state-wide policies on recording whether or not voter order is recorded.

[17] While in theory it should not matter what language is used for displaying the ballot, there was a demonstration provided by Sequoia (not in Kentucky) which accidentally proved that this is an important factor: due to an error in the ballot programming for the demonstration, votes counted in English were recorded correctly, but votes cast in Spanish were ignored.

- While the vendors generally had appropriate locations for use of numbered seals, there was no discussion of the use of those seals in Kentucky counties. While not a flaw in the certification itself, the proper use of seals should be a condition for use of the certified machines.

- None of the certifications included discussions of the risks of Internet connectivity, and why it is critical that none of the systems, including the ballot programming system, ever be connected to the Internet (including any office networks). Two of the vendors (ES&S and Hart) pointed out the advantages their DREs had in not using any form of a network among the components of the system, but did not point out issues of connecting the programming or tallying devices to the Internet.

- While all of the vendors stated that they do not use any form of WiFi networking, there was no effort made to verify that claim, either by physical inspection of the internals of the systems, or by using wireless scanners. In a related point, the vendors were not asked (and did not volunteer) whether they use related technologies which are wireless but not WiFi such as infrared[18], RFID or Bluetooth, any of which might be points of attack. As use of wireless technologies is not covered by the ITA reports, it bears investigation. Professor Shamos notes[19] "There is no legitimate use of wireless communications in voting systems".

- The security of all of the machines appears to be extremely dependent on their never coming in contact with malicious code, as once that occurs there are few defenses or recovery mechanisms. This is sometimes referred to as the "M&M model of security": there is a hard crunchy exterior that protects a soft chewy interior.

ES&S: In addition to the general comments about the certification process above, the ES&S representative was unfamiliar with the Florida report which identified problems with the iVotronic, and in particular was unfamiliar with the problems described in Appendix G (which was redacted from the public version of the document due to the sensitivity of the information).

Additionally, there was no discussion of the known problem with the "smoothing filter" problems[20] in the ES&S iVotronic, and whether that fix has been implemented in the version of the software certified in Kentucky.

[18] The ES&S iVotronic uses infrared for communication between the DRE and the PEB [Personal Electronic Ballot] used to enable the machine. While infrared communications only work at very close distances, this was not considered as part of the certification.

[19] Shamos, slide 16.

[20] The "smoothing filter" is a piece of software in the iVotronic that is used to detect when the screen has been pressed. A problem in this software could lead to long delays between when a voter presses the screen and when the selection appears on the screen. This has been proposed as a possible explanation for the very high undervote rate in the Sarasota County portion of Florida's 13th Congressional District, although the Florida study discounts that possibility.

Finally, there was no discussion of whether ES&S would provide a point-by-point response to the findings of the Florida study.

Hart Intercivic: In addition to the general comments above, I noted the following points:

- The equipment contained numerous physical ports which are points of vulnerability to an attacker. The Hart representative made excellent suggestions that they should be covered with tamper-evident tape. The SBE should verify that these recommendations are in writing, and are followed by all of the counties.

- Hart representatives incorrectly claimed that they are the only vendor to be approved in California without conditions for the November 2007 election[21]. The California Secretary of State noted that the Hart Intercivic 6.2.1 was "found and determined to be defective or unacceptable and its certification and approval for use in subsequent elections in California is immediately withdrawn" subject to a large number of conditions[22].

- Hart representatives did not offer SBE certifiers the opportunity to mark optical scan ballots, nor did any of them request that opportunity.

- Hart representatives stated that they do not intend to provide point-by-point responses to the California study.

- Hart representatives stated that they did not prepare a demonstration of non-partisan and primary elections (required by the Kentucky checklist used by SBE certifiers). There was no questioning on this point by the examiners.

Diebold: In addition to the general comments above, I noted the following points:

- Diebold representatives were highly critical of the California report, noting that there were no compensating controls in place which might have prevented some of the attacks. While this statement is correct, the compensating controls are different in each county in California (as noted in the California reports themselves), and indeed in each county in Kentucky. Hence, any reliance on compensating controls would reduce the generality of the results, and might give false assurances if some of the expected countermeasures are not in place.

[21] The California Secretary of State's decision on Hart Intercivic 6.2.1 may be found at http://www.sos.ca.gov/elections/voting_systems/ttbr/hart.pdf.

[22] "Withdrawal Of Approval Of Hart Intercivic System 6.2.1 DRE & Optical Scan Voting System And Conditional Re-Approval Of Use Of Hart Intercivic System 6.2.1 DRE & Optical Scan Voting System", California Secretary of State Debra Bowen, August 3 2007, http://www.sos.ca.gov/elections/voting_systems/ttbr/hart.pdf, page 5.

- Diebold representatives provided a purported point-by-point response to the California report, which they said will be posted on their web site[23]. The Diebold response agreed with a few of the findings, but generally disagreed with their methodologies, especially with respect to the lack of a "blue team" (a defensive team). While Diebold is correct that no blue team was allowed, this is in fact the norm for this type of a test: the goal of the effort is to find a worst-case scenario[24], and then to look at compensating controls that might be imposed.

- There was no demonstration of primary elections (required by the Kentucky checklist used by SBE certifiers). There was no questioning on this point by the examiners.

Recommendations

Based on my expertise in the area of voting systems, I recommend that the Commonwealth of Kentucky take a series of short-term and a series of long-term actions.

Short-term recommendations (before Nov 2007 election)

- The SBE should develop a set of written policies and procedures (P&P) for use in all counties in the Commonwealth for protection of voting machines[25]. The P&P should include:
    - Rules on avoiding network connectivity to prevent viruses or other malicious software from entering the voting systems.
    - Procedures for changing and proper storage of all encryption keys and passwords.
    - Procedures for installing seals in all appropriate places on the voting machines, and more importantly, *checking* that the seals are unbroken at appropriate intervals on election day and after the election is over.
    - Procedures for ensuring that the version of hardware and software in use in each county is the same as that approved through the SBE certification process, to avoid the recent problems where Diebold installed uncertified software in Jefferson County.

[23] As of the date of this report, the Diebold report has not been posted. The copy provided to the Attorney General's office was under a non-disclosure agreement. As I expect my report to become public, I have not included any proprietary information from Diebold's response in this report.

[24] As noted in the California report, they were unable to complete their work due to an extremely compressed timeline. While Diebold has stated that the effort available to the California team was excessive, it is much less than would be available to a determined adversary trying to change election results. As noted in the California report, "the results presented in this study should be seen as a 'lower bound'; all team members felt that they lacked sufficient time to conduct a thorough examination, and consequently may have missed other serious vulnerabilities".

[25] Such policies and procedures may already exist, but I have been unable to identify any descriptions thereof.

- The SBE should follow the recommendations of the California Secretary of State in her decertification/recertification memos for proper P&P, pollworker training, logs, etc.
- The SBE should require that Hart and Diebold provide all fixes to Kentucky that they provide to California as a result of the recertification process.
- The SBE should require that ES&S provide all fixes to Kentucky that they provide to Florida as a result of that study.
- The SBE should require that all three vendors provide all fixes to Kentucky that they provide to other states as a result of future studies[26].

Long-term recommendations (before Nov 2008 election)

- The SBE certification process should be dramatically improved, including:
    - Providing significant additional time for the certification review, including time for the SBE members to use the machine without the presence of vendor staff.
    - Requiring the participation of one or more individuals with both voting and computer security expertise.
    - Requiring the use of common technologies such as network "sniffers" to detect the presence of wireless communications.
    - Including additional requirements for security as part of the certification checklist.
    - Including the central programming and tallying system as part of the certification process.
    - Paying greater attention to privacy concerns, including violation of privacy via use of continuous paper tape.
    - Paying greater attention to multi-language support, if applicable in Kentucky.
    - Adding an expert in the area of accessibility to the certification team.
- The SBE should require that all vendors requesting certification in Kentucky provide the source code and design documents for their software for use by the SBE or its designated representatives as part of future studies. This should include all necessary protections to prevent disclosure of proprietary information, but must not preclude the SBE from hiring independent experts who sign non-disclosure agreements.

[26] For example, Ohio is in the process of performing a similar study to California and Florida.

- Legislation should be considered to give the SBE the right to demand recertification at periodic intervals, rather than the current model where once certified, a machine cannot be decertified unless the vendor submits a newer version. This will allow the SBE to reexamine voting equipment as more information is learned about equipment risks and vulnerabilities.

- The state should begin moving away from DREs and towards optical scan systems with use of marking devices such as the ES&S Automark. This will bring Kentucky in line with the proposed Federal legislation which will require such changeover, although the timeline is currently unclear.

- The state should establish policies and procedures for mandatory random audits[27] of all elections to establish the accuracy of the machine counts. This can be done on both optical scan systems and those DREs that include a paper trail. The selection of machines and jurisdictions for random audit should follow recommendations from the Brennan Center and the Samuelson School[28].

- The state should establish policies & procedures for use of recounts using the optical scan ballots and DRE paper trails, rather than relying on the machine-generated totals.

- The SBE should work with the counties in developing in-house expertise in programming the ballots. At present, many if not all counties rely on the vendors to perform the ballot programming, which is a risky practice.

Conclusion

I want to commend Mr. Smotherman, the appointed computer science expert. He was clearly well prepared for the meeting, having reviewed the California and Florida reports, and asked good questions of the vendor representatives. Unfortunately he, like all members of the committee, was severely constrained by time, as all three systems were to be reviewed in a single day's meeting. Hence, neither he nor anyone else was able to obtain the depth of information that is necessary before making such an important decision.

The Commonwealth of Kentucky has many strengths in its voting certification process, including dedicated and hardworking members of the staff at the State Board of Election. By following the

[27] The term "random audit" in this context means a selection of random precincts at every election, and a manual comparison of the vote totals generated by the voting equipment with physical paper ballots (be they optical scan or VVPAT). This should occur regardless of whether there are any observed irregularities, to detect accidental or intentional errors in the voting equipment totals. The specific number of precincts required to obtain desired confidence levels is a mathematical function based on the number of votes and other factors which are described in the Brennan/Samuelson report.

[28] "Post-Election Audits: Restoring Trust In Elections", Brennan Center for Justice at New York University School of Law and the Samuelson Law, Technology & Public Policy Clinic at the University of California, Berkeley School of Law (Boalt Hall), http://www.brennancenter.org/dynamic/subpages/download_file_50227.pdf

recommendations in this report, Kentucky will increase the confidence its voters have in the security and reliability of their voting systems.

If I may be of further assistance, please do not hesitate to contact me.

Sincerely,

Jeremy Epstein
4575 Forest Drive
Fairfax VA 22030

CC: Pierce Whites, Deputy Attorney General
Jennifer Hans Black, Assistant Attorney General