



COMMONWEALTH OF KENTUCKY
OFFICE OF THE ATTORNEY GENERAL

GREGORY D. STUMBO
ATTORNEY GENERAL

CAPITOL BUILDING, SUITE 118
700 CAPITOL AVENUE
FRANKFORT, KY 40601-3449
(502) 696-5300
FAX: (502) 564-2894

November 15, 2007

Commissioner Donetta Davidson
Chairwoman
U.S. Election Assistance Commission
1225 New York Ave. NW, Suite 1100
Washington, DC 20005

RE: Submission of Reports on Kentucky's Electronic Voting Systems

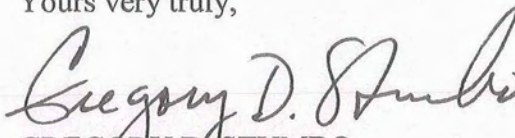
Dear Chairwoman Davidson:

I am pleased to submit to the United States Election Assistance Commission ("EAC") a copy of *Kentucky's Election Voting Systems and Certification Process* (October 23, 2007), comprised of an investigative report by my staff and the expert report of Mr. Jeremy Epstein, an independent consultant on electronic voting systems. I am submitting these reports to be included in the EAC's national clearinghouse of voting system reports.

This report reflects my experience overseeing elections in Kentucky, particularly my 2007 investigation of Kentucky's electronic voting systems and Mr. Epstein's expert recommendations regarding state certifications of these systems. Pursuant to the EAC's 2007 policy on posting reports and studies regarding voting systems, I request that Kentucky's report be added to the EAC's web site and clearinghouse of information.

I thank you for your consideration of this matter.

Yours very truly,


GREGORY D. STUMBO
Attorney General

Enclosure

Cc: Jeremy Epstein
Secretary of State, Trey Grayson



TABLE OF CONTENTS:

INVESTIGATIVE REPORT

Ensuring Your Vote Counts: Kentucky's Electronic Voting Systems

Attorney General Greg Stumbo's Investigative Report

September 18, 2007

<http://ag.ky.gov/NR/rdonlyres/38B944CF-1F47-44D3-82DD-ED46CE0E733B/0/votingsysteminvreport.pdf>

APPENDICES

<http://ag.ky.gov/NR/rdonlyres/834C57D0-4CEF-4FFC-A79C-CD3951918F23/0/votingsysteminvreportappendices.pdf>

EXPERT REPORT

Improving Kentucky's Electronic Voting Systems Certifications

by Jeremy Epstein

September 28, 2007

<http://ag.ky.gov/NR/rdonlyres/1B3F7428-0728-4E83-AADB-51343C13FA29/0/votingexpertletter.pdf>

Biography of Jeremy Epstein



ENSURING YOUR VOTE COUNTS:

KENTUCKY'S ELECTRONIC VOTING SYSTEMS

ATTORNEY GENERAL GREG STUMBO'S

INVESTIGATIVE REPORT

&

EXPERT REPORT

PRESENTED TO

JOINT TASK FORCE ON ELECTIONS, CONSTITUTIONAL AMENDMENTS

AND INTERGOVERNMENT AFFAIRS

October 23, 2007

KEY FINDINGS

- **Public confidence in elections is at an all time low.** Public confidence will be restored when state officials demand secure voting systems. Prompt correction of security failures is a priority requiring cooperation among elected officials.
- **Studies show that the electronic voting systems employed in Kentucky are not secure.** Independent expert reviews of electronic voting systems conducted this year by California and Florida researchers reveal serious security vulnerabilities in voting systems currently employed in Kentucky. Security upgrades must be promptly implemented.
- **Current electronic voting system certification provides no meaningful security review.** Kentucky's existing certification process merely rubber stamps a brief and flawed examination.
- **Isolated components should not be tested apart from the systems in which they operate.** Meaningful certification testing should always consider the performance of each component within its operating system. Individual component testing invites unforeseen system failures.
- **Critical components are not presently tested.** Certain critical voting system components have never been tested or certified at all. These include components which collect and report final ballot totals.
- **No electronic voting systems in Kentucky have been certified by the federal government.** It is up to Kentucky to ensure that voting systems are safe and reliable.
- **Adding a paper trail, without more, fails to address the problem.** Implementation of a voter verifiable paper record (VVPR) or audit trail (VVPAT) may provide some additional security if random audits of official paper ballots are required, but **will not cure the security flaws presently identified in these systems.**
- **Jefferson County's use of a non-certified electronic voting system should have been detected and corrected during normal State oversight procedures.** Properly following existing procedures will ensure that this problem is eliminated in the future.

DOCUMENTED PROBLEMS WITH ELECTRONIC VOTING SYSTEMS

Other States Have Found Significant Problems in the Voting Systems Used in Kentucky. To Protect the Integrity of the Vote and Secrecy of the Ballot, Kentucky Should be an Early Adopter of Improved Voting Systems.

SUMMARY:

The Attorney General brought this matter to the State Board of Election's attention so that Kentucky could benefit from improvements to voting systems implemented in other states. See: Letter of August 7, 2007 to Secretary Trey Grayson. The Attorney General requested a reexamination of certain Kentucky voting systems following an independent review by the California Secretary of State which found numerous security flaws.

As California and other states succeed in demanding fundamental improvements to voting systems, Kentucky must not be left behind. The State Board of Elections should insist that Kentucky voters receive the same protections offered to voters in sister states. The aim is to protect the integrity of the vote and the secrecy of the ballot. The Attorney General will offer legal assistance to accomplish this crucial goal.

COMMENTS:

In May, 2007, California Secretary of State Debra Bowen initiated a comprehensive study of all electronic voting systems certified in California. The goal of this top to bottom review was to address the public's lack of confidence in these systems. The study examined whether the voting systems should be (1) left alone, (2) allowed only with additional protections, or (3) decertified and banned from use.

The University of California provided independent researchers to test security measures, (the "Red Team") and system soft ware, (the "source Code Review Team".) The results of the testing were so dismal that California **decertified** all the systems reviewed. According to Secretary Bowen, "the expert reviewers demonstrated that the physical and technological security mechanisms provided by the vendors for each of the voting systems analyzed were inadequate to ensure accuracy and integrity of the election results and of the systems that provide those results." See: *Withdrawal of Approval of Hart Intercivic System 6.2.1 DRE and Optical Scan Voting System* (August 3, 2007) and *Withdrawal of Approval of Diebold Election Systems, Inc. GEMS 1.18.24/AccuVote-TSX/AccuVote-OS DRE & Optical Scan Voting System* (August 3, 2007). Secretary

Bowen agreed to **conditionally** recertify the voting systems **if the vendors made significant technical and procedural modifications within sixty (60) days.**

The voting systems tested included two (2) systems heavily used in Kentucky: (1) the Hart InterCivic eSlate Voting System, software version 6.2.1 and its related components, certified by the State Board of Elections on December 19, 2006; and (2) Diebold Election Systems, Inc.'s¹ AccuVote Optical Scan ("OS") (model D) with firmware version 1.96.6, Voter Card Encoder 1.3.2, AccuVote-OS Central Count firmware version 2.0.12, Key Card Tool 4.6.1 and VCProgrammer 4.6.1, which were all certified on August 16, 2005², and AccuVote-TSX DRE (Model D) Touch Screen (certified on September 19, 2006) with Ballot Station firmware version 4.6.4 (certified on March 21, 2006).

The California Source Code Review Team found multiple software shortcomings in these systems established security threats. Source Code reviewers also determined that both systems contained enough raw data to reconstruct voting and compromise the secrecy of the ballot. Specific findings are detailed in the *Withdrawal of Approval* Orders, attached as Exhibit A.

The California "Red Team" study revealed multiple vulnerabilities in both systems that could compromise the accuracy, secrecy, and availability of the voting systems. See: *Overview of Red Team Reports* available at http://www.sos.ca.gov/elections/voting_systems/ttbr. The two most significant findings were:

- (1) That the Hart voting system was open to remote eavesdropping and capture of the audio narration of a ballot (which is a design feature for use by disabled voters), potentially violating the secrecy of the ballot; and
- (2) That Diebold Red Team members, without access to the source code, were able to violate the physical security of *all aspects* of the AccuVote TSX DRE under conditions normal for a polling place and with the use of typical office tools.

Other "Red Team" findings are detailed in Secretary Bowen's *Withdrawals of Approval*.

¹ Now Premier Election Solutions, Inc.

² The SBE did not examine or certify the Diebold election management system, GEMS software, version 1.18.24. See: Letter dated August 17, 2005, describing GEMS v. 1.18.24 as "Ballot Origination Software," over which the SBE stated it had no authority. The GEMS election management system is not limited to ballot design, but rather it works in tandem with the other Diebold components and, in addition to creating ballots, accumulates summary data from voting devices and reports final election results. The California study analyzed the GEMS election management system and found serious security flaws that could affect election outcomes.

Kentucky Should Adopt California's Requirements for Re-Certification.

SUMMARY:

Specific improvements have been identified to make Kentucky's voting systems less vulnerable to tampering.

COMMENTS:

After decertifying the deficient electronic voting systems, Secretary Bowen provided imposed specific procedural safeguards for their use and required the relevant vendors to make specific changes to the hardware and operating platforms of the electronic voting systems. California required the following improvements:

- Re-flashing or re-installing the firmware or software in all voting system components;
- Removing, blocking or disabling access to unneeded ports on the machines;
- Hardening the configuration of the hardware and operating platforms' servers to improve security;
- Development and submission by the vendor of a plan and procedures for the timely identification, vendor testing and secure distribution and application of vendor-approved security updates;
- Development and submission by the vendor of uniform security requirements and use procedures for election officials;
- Banning all modem or wireless connections, regardless of their purpose, in order to prevent connection to an unauthorized computer or network or to the Internet;
- Adding security seals and chain-of-custody provisions; and
- Development and submission by the vendor of uniform requirements and use procedures for programming, pre- and post-election logic and accuracy testing, transporting and operating voting equipment to prevent or detect unauthorized access

Currently, Secretary Bowen is investigating a third vendor active in Kentucky, Election Systems & Software ("ES&S"), for selling non-certified electronic voting machines in California. See: Public Notice of Hearing available at <http://www.lrc.ky.gov/KRS/117-00/CHAPTER.HTM>. Voting systems manufactured by ES&S are used in approximately 20 counties in Kentucky. This investigation will be monitored.

Florida and Ohio Reviews of Electronic Voting Systems Used in Kentucky Have Also Uncovered Serious Security Flaws

SUMMARY:

In response to numerous complaints, lawsuits and public concern regarding the integrity of electronic voting systems, the Secretaries of State of Florida and Ohio have commissioned independent studies of electronic voting systems.

One Florida review found 125 software security flaws and successfully demanded that the manufacturer repair the flaws within ten (10) days.

Ohio's initial findings will be released this Thursday, and should be closely reviewed by the State Board of Elections.

COMMENTS:

In Florida, Governor Charlie Crist is actively reviewing electronic voting systems employing touch-screen voting and is advocating their eventual ban. See: *Florida Acts to Eliminate Touch-Screen Voting System*, NYT (May 4, 2007). Florida Secretary of State Kurt S. Browning commissioned Florida State University's Security and Assurance in Information Technology ("SAIT") Lab to conduct a study of the touch-screen systems used in Sarasota County and manufactured by Election Systems & Software (ES & S). The study identified several software vulnerabilities in the iVotronic firmware affecting the security of the system. See: *Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware* (February 23, 2007), available at <http://election.dos.state.fl.us/pdf/FinalAudRepSAIT.pdf>. The ES&S iVotronic machines are used in approximately 20 Kentucky counties.

Florida Secretary of State Browning also commissioned a study of the most recent Diebold-OS Voting System and companion GEMS v. 1.18.25 election management software. The independent SAIT report, issued July 27, 2007, identified more than 125 software flaws affecting the security of the system. See: *Software Review and Security Analysis of the Diebold Voting Machine Software* (SAIT July 27, 2007), Appendix A Flaw List, available at: <http://election.dos.state.fl.us/pdf/SAITreport.pdf>. Secretary Browning immediately demanded that Diebold make all necessary modifications and withheld certification until they were completed and reviewed. See: Letter from Secretary Browning to Diebold dated July 31, 2007 available at: <http://election.dos.state.fl.us> **Diebold complied in ten (10) days.** See: Letter from Secretary Browning to Diebold dated August 10, 2007 available at: <http://election.dos.state.fl.us>.

On June 18, 2007, Ohio Secretary of State Jennifer Brunner launched an Evaluation & Validation of Election-Related Equipment, Standards & Testing ("EVEREST") project by issuing a request for proposals for an independent risk assessment study of Ohio voting systems, which (like Kentucky) currently include Hart, Diebold and ES&S DRE voting systems. See: RFP, Consulting & Testing Services – Risk Assessment Study, available at <http://www.sos.state.oh.us/sos/info/EverestFAQ.pdf>. The initial goal date for results of this study is scheduled for September 20, 2007.

There Are No Federally-Certified Electronic Voting Systems

SUMMARY:

No federal agency has certified Kentucky's voting systems. It is up to Kentucky to demand reliability, accuracy and security by conducting meaningful certifications.

COMMENTS:

Prior to January 1, 2007, no federal agency certified electronic voting systems. Before the enactment of the Help America Vote Act of 2002 (HAVA), the Federal Election Commission ("FEC") had exclusive authority over federal elections. After passage of HAVA, the FEC promulgated voluntary standards for voting systems (VSS 2002), but had no method of certifying these systems. Therefore, the National Association of State Election Directors ("NASED") stepped in to qualify those electronic voting systems that met the VSS 2002 as determined by third-party laboratories paid by the vendors to review their products.

HAVA also created the Election Assistance Commission ("EAC"), a separate federal authority charged with the oversight of federal electoral procedures and processes, including the accreditation of voting system test laboratories and the implementation (by 2007) of a voluntary certification program for voting systems vendors. The EAC has completed its accreditation of laboratories, but these laboratories still rely on the vendors for payment only after they approve the vendors' systems. The EAC is currently conducting certifications of vendors that meet the voluntary voting systems guideline for 2005 (VVSG 2005) as determined by an accredited laboratory. As of the date of this memorandum, there are no federally certified voting systems.

The VVSG 2005 was promulgated by the EAC in conjunction with the National Institute for Science & Technology ("NIST"). The NIST is preparing to send the EAC a new set of guidelines – VVSG 2007, which require expanded usability & accessibility in voting devices, open source software (as opposed to the proprietary systems now in use), independent voter-verifiable records (distinguishable from the voter-verifiable paper audit trail – VVPAT – now in use), expanded security coverage and end-to-end testing for accuracy, security and reliability. *See: www.nist.gov/VVSG-0807*. At a recent meeting of the Technical Guidelines Development Committee (TGDC), members estimated that ultimate approval of VVSG 2007 by the EAC would not occur until 2009 at the earliest.

At this time, certification and review at the state level is the only measure of reliability, accuracy and security for electronic voting systems and the only means of holding election industry vendors accountable to their voter consumers.

Failed State Oversight Resulted in Jefferson County's Use of Non-Certified Equipment

SUMMARY:

Kentucky's HAVA Plan Requires the State Board of Elections to Oversee The Expenditure of Funds Distributed to The States for the Purchase of Voting Systems. Failure to Follow the Plan Resulted in the Unauthorized Use of Non-Certified Equipment.

COMMENTS:

The Commonwealth of Kentucky, through the office of then-Secretary of State, John Y. Brown III, developed a comprehensive State Plan for implementing HAVA and for managing the federal funds made available to the Commonwealth under the provisions of HAVA. *HAVA State Plan* (2003). The 2003 State Plan required the State Board of Elections to "manage all [HAVA] Title II funds and account for all expenditures, funding levels, program controls and outcomes" *Id.* at p. 13. In order to receive the HAVA funds, counties were to enter into a memorandum of understanding with the Secretary of State and were "to submit semi-annual reports on their performance." *Id.*

According to the Amended State Plan, presented by Secretary of State Trey Grayson in 2006, "the State Board of Elections required each county to send documentation of the purchase of the voting systems or upgrade, which included serial numbers from each component, type of equipment, make and manufacturer of the voting machine or upgrade." *Id.* at p. 6. As of 2006, the State Board of Elections should have collected data on every component of every voting system purchased or upgraded using HAVA funds.

Had this process been followed, non-certified equipment would never have been in use in Jefferson County. It is essential that the Secretary of State and State Board of Elections recognize and adhere to the essential safeguards provided in the Amended State Plan, rather than denying responsibility for oversight of voting systems.

Jefferson County's Use of Non-Certified Voting Equipment

The investigation showed that Jefferson County was using a voting system not certified by the State Board of Elections. Despite Premier/Diebold's claim that the error was harmless, the OAG immediately sought additional information from Secretary Grayson. Rather than proving the security of the equipment, the Secretary of State's office suggested that the OAG seek statutory changes instead of continuing an investigation of this matter.

While the Attorney General certainly shares the desire of all election officials to hold accountable vendors like Premier/Diebold who fail to comply with the law, evidence gathered does not support Secretary Grayson's contention that there was nothing more that could have been done to prevent this egregious failure. A review of public records reveals the following:

- (1) That on August 23, 2007, the week prior to Diebold's letter, SBE was notified that Jefferson County's electronic voting system included non-certified optical scan units. *See* email from Jefferson County Clerk to Sarah Ball Johnson identifying the Accuvote-2000, version 1.96.4. This startling information was not shared with the OAG, despite being discovered as a direct result of inquiries by this office.
- (2) Pursuant to KRS 117.377(1), SBE should have been notified of the uncertified system in FY 2005 when Jefferson County installed its new electronic voting system. More than \$2.5 million in federal funds from the Help America Vote Act ("HAVA") and \$233,500 in county capital funds were paid to Diebold for the new voting system. *See*: Louisville Metro Capital Improvement Program Summaries.
- (3) Kentucky's 2006 Amended State Plan "required each county to send documentation of the purchase of the voting systems or upgrade, which included serial numbers from each component, type of equipment, make and manufacturer of the voting machine or upgrade." Jefferson County failed to provide documentation to the SBE revealing the use of outdated and non-certified optical scan units, and SBE failed to demand same.

The SBE has clear oversight authority regarding all electronic voting systems in Kentucky. This authority should be used in the future to prevent use of uncertified voting systems.

Shortcomings in Kentucky's Certification Process

Kentucky election law demands the examination and certification of all electronic voting systems prior to their purchase and use in the counties. A voting system that has been approved as in conformity with federal standards must still be certified for use in Kentucky. The OAG discovered the following shortcomings with the certification process:

- (1) The State Board of Elections does not require voting machine examiners to submit their qualifications prior to being selected.
- (2) The State Board of Elections has used as a computer expert a professional with experience in information technology management, but with insufficient experience in software engineering and systems security, and no experience in electronic voting systems prior to his work for Kentucky.
- (3) The State Board of Elections provides each examiner with a checklist, containing only a recitation of the statutory language of KRS 117.381. No guidance concerning in-depth testing and examination is offered, and no system is in place to allow such review.

- (4) The State Board of Elections permits vendors to submit isolated components of voting systems for certification, rather than testing systems as a whole. This invites system failures under real world conditions.
- (5) The State Board of Elections declines to examine and certify key components of voting systems, including the Premier/Diebold's GEMS election management system. This omits any review of critical components that are highly vulnerable to abuse and manipulation. As a result of this lack of testing and certification, essential elements of Kentucky's voting systems that collect and report ballot totals are not subject to independent evaluation at all. Effective examination and certification of these neglected components should proceed immediately.

These shortcomings in the certification process permit vendors to submit the most basic information and anticipate that the State Board of Elections will rubber stamp their certification as long as their own financed testing shows that they comply with the minimum federal requirements. Kentucky voters deserve effective, independent testing overseen by state officials to ensure reliable, accurate and secure voting systems.

THE ATTORNEY GENERAL'S RECOMMENDATIONS:

Immediate action is necessary to preserve public confidence in elections. The Attorney General proposes that the State Board of Elections take the following remedial actions to address identified issues:

- Require vendors to immediately correct or mitigate identified flaws in electronic voting systems at no additional cost to Kentucky taxpayers. State certification should be conditioned on vendor compliance, as required under KRS 117.381.
- Incorporate security and accuracy procedures and protocols recommended by the California and Florida studies into the training offered to counties and poll workers.
- Require counties to accurately and fully report the purchase and installation of electronic voting systems as required under state law.
- Reform the certification process for electronic voting systems by appointing independent examiners with specific experience in electronic voting systems and security protocols and by revising the examiner checklist to create a meaningful review of electronic voting systems, and requiring adequate depth of analysis.
- Require that all voting system vendors provide an escrow of all source code, with conditions allowing it to be used for independent assessments while protecting the

vendor's proprietary information. The SBE should use California's language as a model in this regard.

FORTHCOMING EXPERT REPORT OF CERTIFICATION PROCEDURES

The Attorney General thanks the State Board of Elections for opening yesterday's certification process to review by the OAG's independent expert. A detailed report of the Attorney General's findings will be provided within ten (10) days. The SBE should not, however, delay implementing the recommendations made herein.

APPENDICES

- Appendix I AG's Request for Reexamination & related correspondence
- Appendix II California Secretary of State's Withdrawals of Approval
- Appendix III *Newsweek* Editorial: Electronic Voting Machines Aren't Ready for '08
- Appendix IV Documents relating to Jefferson County's use of non-certified voting system
- Appendix V Kentucky Requirements for Voting Systems



COMMONWEALTH OF KENTUCKY
OFFICE OF THE ATTORNEY GENERAL

GREGORY D. STUMBO
ATTORNEY GENERAL

CAPITOL BUILDING, SUITE 118
700 CAPITOL AVENUE
FRANKFORT, KY 40601-3449
(502) 696-5300
FAX: (502) 564-2894

September 18, 2007

URGENT

Via hand-delivery

Secretary of State Trey Grayson
Chairman, State Board of Elections
Suite 152, State Capitol
700 Capitol Avenue
Frankfort, Kentucky 40601

RE: Jefferson County Uncertified Voting System--
Incorrect Diebold Voting System Submitted for Examination

Dear Secretary Grayson:

In an effort to correct the failure to use certified voting machines in Jefferson County, the State Board of Elections directed the manufacturer, Premier/Diebold, to submit its product for additional examination on September 17, 2007. During this examination, my staff observed that Premier/Diebold apparently presented the wrong machine for certification.

The device submitted for review was the AccuVote Optical Scan ("OS") Model D firmware. In its letter dated August 27, 2007, Premier/Diebold attested to you and the SBE that Jefferson County's non-certified OS units would be upgraded with this Model D firmware.

According to the testimony of Premier/Diebold to the SBE's examiners, this is not the case. Premier/Diebold merely patched the old AccuVote OS Model A firmware units with a series of corrections, claiming to transform the Model A units into Model D units. Yet what was presented to your examiners was not an adapted Model A unit, as updated in Jefferson County, but rather a brand new Model D unit. The integrity of voting machines actually used in elections remains in doubt.

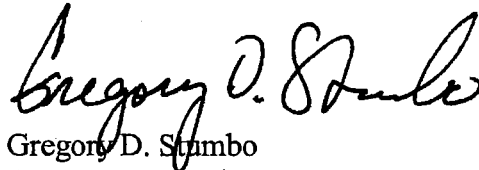
The failure of Premier/Diebold to present for certification the equipment it has provided to Jefferson County negates any certification that the SBE may finalize today. Jefferson County officials would again confront either purchasing new equipment that has been certified or knowingly using non-certified equipment currently available in violation of state law.



Secretary Trey Grayson
RE: Examination of Diebold Voting System
September 19, 2007
Page 2 of 2

Therefore, I recommend that the SBE immediately require Premier/Diebold to correct this error either by submitting a modified Model A unit for certification or agreeing to immediately provide the appropriate Model D upgrades to Jefferson County.

Sincerely,

A handwritten signature in black ink, appearing to read "Gregory D. Stumbo". The signature is written in a cursive, flowing style.

Gregory D. Stumbo
Attorney General

C: Sarah Ball Johnson

APPENDIX I



COMMONWEALTH OF KENTUCKY
OFFICE OF THE ATTORNEY GENERAL

GREGORY D. STUMBO
ATTORNEY GENERAL

CAPITOL BUILDING, SUITE 118
700 CAPITOL AVENUE
FRANKFORT, KY 40601-3449
(502) 696-5300
FAX: (502) 564-2894

August 7, 2007

Via hand-delivery

Secretary Trey Grayson
Chairman
State Board of Elections
700 Capitol Avenue, Suite 152
The Capitol Building
Frankfort, KY 40601

RE: Request for Reexamination of Electronic Voting Systems

Dear Secretary Grayson:

Pursuant to my authority under KRS 15.243 to enforce the state's election laws, I am requesting that the State Board of Elections reexamine the Hart InterCivic Direct Record Electronic ("DRE") Precinct Voting Systems and the Diebold Accuvote-TSX DRE and Optical Scan ("OS") Voting Systems. On August 3, 2007, pursuant to Executive Order, the California Secretary of State, Debra Bowen, legally decertified these systems finding them "to be defective or unacceptable." See enclosed, *Withdrawal of Approval of Hart InterCivic System 6.2.1 DRE* (August 3, 2007) and *Withdrawal of Approval of Diebold Election Systems, Inc.* (August 3, 2007). The Hart InterCivic DRE Voting System 6.2.1 or previous versions of this system are employed in 96 of 120 counties in Kentucky. The Diebold Accuvote-TSX DRE and OS Voting Systems are used in Jefferson County, the most populous county in Kentucky.

Beginning in May, 2007, Secretary Bowen ordered an independent top-to-bottom review of all electronic voting systems employed in California. As Secretary Bowen stated, "the Help America Vote Act [HAVA] ... pushed many counties into buying electronic voting systems that...were not properly reviewed or tested to ensure that they protected the integrity of the vote."

Secretary Bowen ordered this review based on public concern over electronic voting systems, even though the electronic voting systems in California were already required to provide verified voting paper audit trails ("VVPAT"), which Kentucky currently lacks. Experts with the University of California at Berkeley and Davis issued reports identifying serious security vulnerabilities in all the voting systems they tested,



Secretary Trey Grayson, Chair

State Board of Elections

August 7, 2007

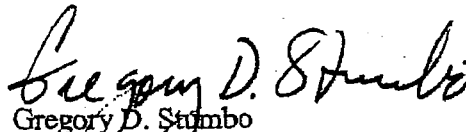
RE: Request for Reexamination of Electronic Voting Systems

Page 2

including the Hart and Diebold DRE systems. The researchers determined that these vulnerabilities could affect the accuracy of voting and compromise ballot secrecy. Access to the specific reports with detailed analysis of the vulnerabilities identified is available online at: http://www.sos.ca.gov/elections/elections_vsr.htm.

At a minimum, the California study and the decertification of these electronic voting systems jeopardize public confidence in the systems used to conduct elections in Kentucky. Therefore, I request that the State Board of Elections immediately order a reexamination of these voting systems pursuant to KRS 117.379 to ensure that they comply with the statutory requirements for electronic voting systems, including ensuring a secret ballot, and with the Kentucky Constitution's guarantee of free and fair elections.

Sincerely,


Gregory D. Stumbo
Attorney General

Enclosures

Cc: J. Allen Eskridge, III
Sarah Ball Johnson

2007-01017



TREY GRAYSON
SECRETARY OF STATE

COMMONWEALTH OF KENTUCKY
OFFICE OF THE SECRETARY OF STATE

SUITE 152, STATE CAPITOL
700 CAPITAL AVENUE
FRANKFORT, KY 40601-3493
(502) 564-3490
FAX (502) 564-5687
WEBSITE: WWW.SOS.KY.GOV

August 7, 2007

The Honorable Greg Stumbo
Office of the Attorney General
The Capitol, Suite 118
700 Capitol Avenue
Frankfort, Kentucky 40601-3449



Dear General Stumbo:

Thank you for your letter of August 7, 2007 concerning California Secretary of State Debra Bowen's recent actions regarding voting systems. I appreciate your interest in our elections and have enjoyed a good working relationship with your office on enforcement of our state's election laws.

As you know, electronic voting systems have been used in most Kentucky counties starting in the mid-1980's without any known security breaches. All systems in use in Kentucky today were unanimously certified by the State Board of Elections pursuant to KRS 117.379 and comply with the federal voting system guidelines in place at the time of certification. Counties make their own decisions about which certified voting systems to purchase.

The State Board is constantly certifying new versions of these voting systems as upgrades are made to the systems as well as new voting system guidelines are adopted. Currently, all voting systems used in Kentucky meet the 2002 federal voting system guidelines, the most recent set of guidelines to which any machines are certified in this country.

The State Board of Elections and I have been monitoring news reports for the past couple of years of potential security flaws with electronic voting systems, especially the newer electronic voting systems mandated by the 2002 Help America Vote Act (HAVA). These systems were designed so that disabled voters, such as those with visual or motor skill disabilities, could vote without assistance. In addition, the systems were purchased by counties mandated by HAVA to replace old lever machines, which were vulnerable to tampering and failure. The vast majority of votes in Kentucky, however, are cast on the older, electronic voting systems.



AN EQUAL OPPORTUNITY EMPLOYER M/F/D

In particular, I have been closely following Secretary Bowen's review from its inception and read the review in its entirety when it was released a few weeks ago, as well as much of the commentary – positive and negative – concerning the review as well as Secretary Bowen's actions taken last Friday.

Obviously, I am concerned about the system vulnerabilities found in Secretary Bowen's review, as well as those found in prior studies over the past couple of years. I am glad that you now share these concerns.

However, I find it misleading and irresponsible your letter states that Secretary Bowen decertified voting systems without stating that Secretary Bowen actually recertified all the voting systems that are used in Kentucky for use in California elections.

In her recertification, she asked for additional safeguards to be taken to insure that machines are not vulnerable. In Kentucky, we already have developed and implemented many safeguards to minimize or eliminate any potential vulnerabilities. Prior to every election, the State Board of Elections works with County Clerks to develop and share best practices to insure that our voting systems are secure and accurate. The State Board of Elections staff then trains county clerks, who in turn train precinct election officers, on these procedures.

For these reasons I feel compelled to note the observation made in the *Los Angeles Times* by Los Angeles County Registrar-Recorder Conny McCormack that the study "was akin to testing the security of your money in a bank with unlocked doors, with no security guards or even bank tellers in sight and the bank's vault wide open." Our poll workers are the bank tellers and security guards on Election Day. We will continue to train them well.

As you may know, I have been leading the effort in Kentucky to require voter verified paper records (VVPR), not just paper receipts, to be used in Kentucky. Currently, Jefferson County voting systems produce a VVPR, while Warren, Graves and Boyle Counties tested VVPR during the May primary. In fact, I was the first elected official in Kentucky to call for VVPR across the Commonwealth.

Our office encouraged State Representative Larry Clark to introduce a bill making VVPR mandatory in the last General Assembly session and have worked to free up approximately \$15 million of our remaining HAVA funds to help the counties purchase such systems. I discussed the broad outlines of this plan this summer at the Judge-Executives and Magistrates/Commissioners Conference as well as during over a dozen visits to County Clerk offices over the past couple of weeks.

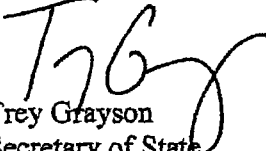
In fact, last week, I shared details of this plan with an office visit with Chris Waugh, County Clerk in your own Floyd County. Many clerks are excited about the availability of these funds and will likely take advantage of this offer for next year's elections.

I will discuss with our State Board members and our State Board of Elections staff your request that we reexamine our voting systems. I have no doubt that the systems will comply with Kentucky law since they have already been examined and certified by the State Board of Elections. In fact, the most recent version of the Hart InterCivic system was examined and certified by the State Board of Elections December 15, 2006. I will be sure to let you know how the State Board of Elections decides to proceed.

It disappoints me that your letter and press release might cause Kentucky voters to have unnecessary doubts about our election systems. Your assertion that we are using voting systems in Kentucky that are no longer certified by California is misleading and irresponsible. As the state's chief law enforcement official, you should know the power of your words and deeds. Your headline chasing has consequences.

The State Board of Elections and election administrators across Kentucky have been working for years to insure the voters have confidence in our system. We will not let you undermine these efforts.

Sincerely,



Trey Grayson
Secretary of State
Chairman, State Board of Elections
Commonwealth of Kentucky



COMMONWEALTH OF KENTUCKY
OFFICE OF THE ATTORNEY GENERAL

GREGORY D. STUMBO
ATTORNEY GENERAL

CAPITOL BUILDING, SUITE 118
700 CAPITOL AVENUE
FRANKFORT, KY 40601-3449
(502) 696-5300
FAX: (502) 564-2894

August 7, 2007

Via hand-delivery

Secretary Trey Grayson, Chairman
State Board of Elections
700 Capitol Avenue, Suite 152
Frankfort, KY 40601

RE: Request for Reexamination of Electronic Voting Systems

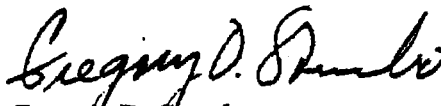
Dear Secretary Grayson:

Thank you for your prompt response to my request for a reexamination of electronic voting systems in Kentucky. Please be advised that your letter of August 7, 2007 contains material errors.

- First, the California Secretary of State Debra Bowen granted a conditional re-approval of use of the Hart and Diebold-manufactured voting systems only upon the companies' correction of the technological and security flaws identified. I'm sure you agree that Kentucky voters deserve this same degree of protection.
- Second, as I detailed in my initial letter, the verified voting paper audit trail ("VVPAT") in place in California was considered by researchers, but was found lacking as a satisfactory method of correcting security flaws in the voting systems. Put simply, your suggestion for a paper record doesn't solve the grave problems identified.
- Third, the new versions of the Hart and Diebold systems were in fact submitted to researchers after the California study was initiated, and it was these new versions that were found to be "defective or unacceptable." The older versions were voluntarily withdrawn from the list of certified systems. Thus, the Board's 2006 certifications must be reexamined in light of this new evidence.

The compelling findings of the California study demand immediate attention. Kentucky can ill afford not to examine this emerging threat, and impugning my motives isn't getting the job done any faster. I hope to continue our good working relationship by assisting you and the State Board of Elections in taking immediate action to protect the voters of Kentucky.

Sincerely,


Gregory D. Stumbo
Attorney General

C: J. Allen Eskridge, III
Sarah Ball Johnson

AN EQUAL OPPORTUNITY EMPLOYER M/F/D





COMMONWEALTH OF KENTUCKY
OFFICE OF THE ATTORNEY GENERAL

GREGORY D. STUMBO
ATTORNEY GENERAL

CAPITOL BUILDING, SUITE 118
700 CAPITOL AVENUE
FRANKFORT, KY 40601-3449
(502) 696-5300
FAX: (502) 564-2894

August 8, 2007

Mr. Greg L. Burt
President and CEO
Hart InterCivic, Inc.
P.O. Box 80649
Austin, TX 78708

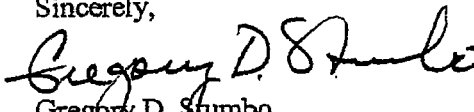
Re: Hart InterCivic System 6.2.1 DRE and prior versions in use in the
Commonwealth of Kentucky

Dear Mr. Burt:

As the public officer authorized to initiate civil and criminal investigations necessary to enforce Kentucky's election laws, I have followed the "Top-to-Bottom Review of Voting Systems" conducted by the California Secretary of State with great interest. Security and privacy issues identified by that review which lead to the Withdrawal of Approval of the Hart InterCivic 6.2.1, and the conditional re-approval of that system entered August 3, 2007, are of particular concern because 96 of the 120 counties in the Commonwealth of Kentucky use the Hart InterCivic System 6.2.1 DRE or prior versions of that system.

Based upon the August 8, 2007 press release issued by Hart InterCivic entitled "Long Beach Election System Recertified for Use in 2008 and Beyond," I understand that Hart will "undertake additional modifications and procedures" mandated by California's Secretary of State as a condition for recertification of the system. Given the heavy reliance the Commonwealth of Kentucky has placed on the Hart InterCivic voting systems in the conduct of its elections, I call upon Hart to immediately implement in Kentucky all modifications and security upgrades necessary to correct the vulnerabilities identified by California. With the election fast approaching, I request the courtesy of a prompt response.

Sincerely,


Gregory D. Stumbo
Kentucky Attorney General





COMMONWEALTH OF KENTUCKY
OFFICE OF THE ATTORNEY GENERAL

CAPITOL BUILDING, SUITE 118
700 CAPITOL AVENUE
FRANKFORT, KY 40601-3449
(502) 696-5300
FAX: (502) 564-2894

GREGORY D. STUMBO
ATTORNEY GENERAL

August 8, 2007

Mr. Dave Byrd, President
Diebold Election Systems, Inc.
1253 Allen Station Parkway
Allen, TX 75002

Re: Diebold AccuVote- TSX DRE and OS Voting Systems in use in the
Commonwealth of Kentucky

Dear Mr. Byrd:

As the public officer authorized to initiate civil and criminal investigations necessary to enforce Kentucky's election laws, I have followed the "Top-to-Bottom Review of Voting Systems" conducted by the California Secretary of State with great interest. Security and privacy issues identified by that review which led to the Withdrawal of Approval of the AccuVote-TSX and AccuVote-OS DRE and Optical scan Voting System, and the conditional re-approval of those systems entered August 3, 2007, are of particular concern because those voting systems are in use in Louisville, Kentucky's most populous city.

Given the heavy reliance the Commonwealth of Kentucky has placed on the Diebold voting systems in the conduct of its elections, I call upon Diebold to immediately implement in Kentucky all modifications and security upgrades necessary to correct the vulnerabilities identified by California. With the election fast approaching, I request the courtesy of a prompt response.

Sincerely,

Handwritten signature of Gregory D. Stumbo in black ink.
Gregory D. Stumbo
Kentucky Attorney General





STATE BOARD OF ELECTIONS

Trey Grayson
Chairman
Secretary of State

140 Walnut Street
Frankfort, Kentucky 40601-3240
Phone: (502) 573-7100
Fax: (502) 573-4369
www.elect.ky.gov

Sarah Ball Johnson
Executive Director
Sandy Milburn
Assistant Director

August 8, 2007

VIA FACSIMILE (512) 252-6556 & U.S. Mail

Mr. Greg L. Burt
President and CEO
Hart InterCivic, Inc.
P.O. Box 80649
Austin, TX 78708

Re: Kentucky Voting System Certification Process

Dear Mr. Burt:

We are in receipt of a copy of the August 8, 2007 letter addressed to you from Attorney General for the Commonwealth of Kentucky, Gregory D. Stumbo, calling "upon Hart to immediately implement in Kentucky all modifications and security upgrades necessary to correct the vulnerabilities identified by California." We would like to take this occasion to remind you of the voting system certification process in Kentucky and to ensure that Kentucky law is followed if Hart InterCivic makes any system upgrades or modifications on voting equipment used in Kentucky elections.

Pursuant to KRS 117.379(1) and KRS 117.381(11), the State Board of Elections may only certify voting systems that meet or exceed all Federal Election Commission voting system standards. As you are aware, the Federal Election Commission's duties in certifying voting systems were subsumed by the Election Assistance Commission ("EAC") created by the Help America Vote Act (HAVA). Therefore, the State Board of Elections may only certify voting systems for use in Kentucky that have first been certified by the EAC.

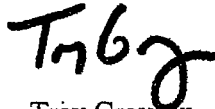
Pursuant to KRS 117.379(4), "when an electronic voting system has been approved any improvement or changes in the system shall render necessary the examination or approval of such system or improvement." Therefore, if Hart InterCivic makes any improvement or change to any of the systems already certified by the State Board of Elections pursuant to the Kentucky Attorney General's request, then Hart InterCivic must bring those

August 8, 2007
Hart InterCivic
Page 2 of 2

improvements or changes before the State Board of Elections again for review and certification. Furthermore, the State Board of Election may not approve the certification of those improvements or changes until the EAC has issued its certification. Most importantly, pursuant to KRS 117.379(3), Kentucky counties, including your customers, cannot use such improvements or changes in Kentucky elections until such certifications have been issued.

Hart InterCivic has consistently followed this process in the past when requesting certification of its products for use in Kentucky. We have every confidence that Hart InterCivic will adhere to these statutory processes in the future.

Sincerely,



Trey Grayson
Secretary of State
Chairman, State Board of Elections
Commonwealth of Kentucky

cc: Roger Baird, President Harp Enterprises
The 96 Kentucky Counties that use the Hart InterCivic Equipment



STATE BOARD OF ELECTIONS

Trey Grayson
Chairman
Secretary of State

140 Walnut Street
Frankfort, Kentucky 40601-3240
Phone: (502) 573-7100
Fax: (502) 573-4369
www.elect.ky.gov

Sarah Ball Johnson
Executive Director

Sandy Milburn
Assistant Director

August 8, 2007

VIA FACSIMILE (214) 383-1596 & U.S. Mail

Mr. Dave Byrd, President
Diebold Elections Systems, Inc.
1253 Allen Station Parkway
Allen, TX 75002

Re: Kentucky Voting System Certification Process

Dear Mr. Byrd:

We are in receipt of a copy of the August 8, 2007 letter addressed to you from Attorney General for the Commonwealth of Kentucky, Gregory D. Stumbo, calling "upon Diebold to immediately implement in Kentucky all modifications and security upgrades necessary to correct the vulnerabilities identified by California." We would like to take this occasion to remind you of the voting system certification process in Kentucky and to ensure that Kentucky law is followed if Diebold makes any system upgrades or modifications on voting equipment used in Kentucky elections.

Pursuant to KRS 117.379(1) and KRS 117.381(11), the State Board of Elections may only certify voting systems that meet or exceed all Federal Election Commission voting system standards. As you are aware, the Federal Election Commission's duties in certifying voting systems were subsumed by the Election Assistance Commission ("EAC") created by the Help America Vote Act (HAVA). Therefore, the State Board of Elections may only certify voting systems for use in Kentucky that have first been certified by the EAC.

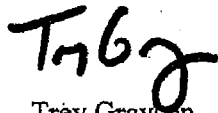
Pursuant to KRS 117.379(4), "when an electronic voting system has been approved any improvement or changes in the system shall render necessary the examination or approval of such system or improvement." Therefore, if Diebold makes any improvement or change to any of the systems already certified by the State Board of Elections pursuant to the Kentucky Attorney General's request, then Diebold must bring those improvements or changes before the State Board of Elections again for review and certification.

August 8, 2007
Diebold
Page 2 of 2

Furthermore, the State Board of Election may not approve the certification of those improvements or changes until the EAC has issued its certification. Most importantly, pursuant to KRS 117.379(3), Kentucky counties, including your customers, cannot use such improvements or changes in Kentucky elections until such certifications have been issued.

Diebold has consistently followed this process in the past when requesting certification of its products for use in Kentucky. We have every confidence that Diebold will adhere to these statutory processes in the future.

Sincerely,

A handwritten signature in black ink, appearing to read "Trey Grayson". The signature is stylized and written in a cursive-like font.

Trey Grayson
Secretary of State
Chairman, State Board of Elections
Commonwealth of Kentucky

CC: Jefferson County Clerk



2007-01085

STATE BOARD OF ELECTIONS

Trey Grayson
Chairman
Secretary of State

140 Walnut Street
Frankfort, Kentucky 40601-3240
Phone: (502) 573-7100
Fax: (502) 573-4369
www.elect.ky.gov

Sarah Ball Johnson
Executive Director

Sandy Milburn
Assistant Director

August 21, 2007

The Honorable Greg Stumbo
Office of the Attorney General
The Capitol, Suite 118
700 Capitol Avenue
Frankfort, Kentucky 40501-3449

Dear General Stumbo:

Please allow this letter to inform you that the State Board of Elections voted today at its regularly scheduled meeting to reexamine the following voting systems, pursuant to KRS 117.379 and 117.381:

1. Any and all Hart InterCivic eSlate DRE voting systems currently in use in Kentucky;
2. Any and all Diebold Accuvote-OS and Accuvote-TSX DRE and related components currently in use in Kentucky; and
3. Any and all ES&S IVotronic voting systems currently in use in Kentucky.

We will inform you of the dates and times of these examinations and invite you and your representatives to attend the examinations. We will also inform you of the results of the reexamination of these voting systems as they occur.

Thank you for your cooperation in this matter. Please feel free to contact us if you have any questions in the interim.

Sincerely,

Trey Grayson
Secretary of State
Chairman, State Board of Elections
Commonwealth of Kentucky



COMMONWEALTH OF KENTUCKY
OFFICE OF THE ATTORNEY GENERAL

GREGORY D. STUMBO
ATTORNEY GENERAL

CAPITOL BUILDING, SUITE 118
700 CAPITOL AVENUE
FRANKFORT, KY 40601-3449
(502) 696-5300
FAX: (502) 564-2894

August 28, 2007

Via hand-delivery

Secretary of State
Trey Grayson
Chairman
State Board of Elections
700 Capitol Ave, Suite 152
Frankfort, KY 40601-3240

Re: **Failure to Certify Jefferson County Voting System**

Dear Secretary Grayson:

Today I received a troubling letter from Diebold Election Systems, (now "Premier Election Solutions, Inc."), stating that Kentucky's largest county has been using uncertified optical scanning units in its electronic voting system, apparently for at least the last three (3) elections. This alarming discovery was made as a direct result of my office's ongoing investigation into irregularities surrounding these voting systems. As Diebold/Premier's letter states, the failure to certify was discovered "in the last few days" as records were reviewed, obviously in response to my investigative demands issued a few days ago.

Please assist my office in determining how this serious breach of statutory protections occurred by responding to the following questions:

1. When did the State Board of Elections and/or your office first become aware of the lack of certification for the Jefferson County electronic voting system?
2. How is it possible that the Accu Vote Optical Scan ("OS") units sold and deployed in Jefferson County were not state-certified?
3. What safeguards and protections will be implemented to prevent future recurrences of this failure?
4. Why did your office fail to advise OAG upon receipt of the Diebold/Premier letter admitting to a lack of certification?



Secretary Trey Grayson
August 28, 2007
RE: Failure to Certify Jefferson County Voting System
Page 2

5. Why were the OS units not upgraded to meet the 2002 Voting Systems Standards ("VSS 2002") promulgated by the Federal Election Commission ("FEC") on April 30, 2002?
6. Were any federal funds authorized under the Help America Vote Act ("HAVA") used to purchase these OS units? Were any federal funds made available to Jefferson County to bring it into compliance with HAVA and VSS 2002? If not, why?

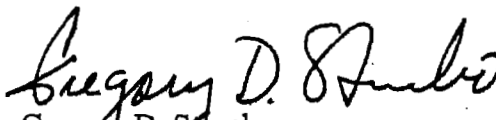
In my August 7, 2007 letter to you, I asked that the State Board of Elections reexamine the particular electronic voting system used in Jefferson County, which has now been discovered to be uncertified. In response you advised that:

All systems in use in Kentucky today were unanimously certified by the State Board of Elections pursuant to KRS 117.379 and comply with the federal voting system guidelines in place at the time of certification.

Obviously, you were in error. It is now necessary for my office to expand its ongoing investigation to include the failure to certify this critical component of a voting system used in the most populous county in Kentucky.

The inconsistency between your assurances and the facts raises serious questions about the quality of the current certification system. I welcome any explanation you may wish to submit as to how Jefferson County was allowed to use an uncertified voting machine for the past three (3) elections outside of the knowledge of the state Board of Elections.

Sincerely,


Gregory D. Stumbo
Attorney General

cc: Sarah Ball Johnson
Kathryn H. Gabhart
Michael Lindroos

2007-01107



Premier Election Solutions, Inc.
P.O. Box 1019
Allen, TX 75013
409 675-8990
fax 214 353-1595
www.premierelections.com

August 27, 2007

Attn: Susan Clark
Jefferson County Clerk's Office
P.O. Box 33033
Louisville, KY 40232-3033
Email: susanclark@jeffersoncountyclerk.org

VIA ELECTRONIC TRANSMISSION

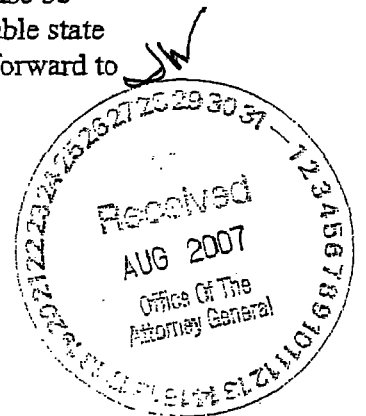
Re: Jefferson County, Kentucky AccuVote-OS Product Version

Dear Susan:

I am writing on behalf of Premier Election Solutions, Inc. (Premier) to make you aware that, within the last few days, a review of our records has revealed that the product version of the AccuVote-OS units deployed in Jefferson County, Kentucky are not a state certified version. The AccuVote-OS product version currently certified in the State of Kentucky is PC 1.96.6 with VSS 2002 compliant hardware. The AccuVote-OS units in use in Jefferson County are running firmware version PC 1.96.4 with hardware that was previously certified by the state but has not yet been upgraded to meet VSS 2002 compliance, which is now required by the State. This earlier version of firmware is, of course, fully federally certified and has been used extensively in several other states; nevertheless it does not have a certification in the State of Kentucky. We have informed the Kentucky Secretary of State's office of this matter.

We deeply regret this error. After an internal review, we have determined that our procedures for verifying state certified versions prior to shipping and implementation were not followed in detail in this case. With your approval, and the State's, Premier will implement a plan to immediately correct this error by upgrading your AccuVote-OS units, hardware and firmware, to the current state certified versions (as identified above) at no cost to the county.

I believe you will find that through Jefferson County's logic and accuracy testing and post-election auditing that there have been no functional or performance issues resulting from the use of the earlier versions of firmware and hardware. However, please be assured that Premier's policy is to provide systems that fully meet all applicable state certification requirements. Again, we apologize for this oversight and look forward to working with you to schedule an upgrade of your AccuVote-OS equipment.



If you have any questions, please contact me at on my cell phone (214.280.6464.)

Sincerely,

A handwritten signature in black ink, appearing to read "Ian S. Piper". The signature is stylized with large, overlapping loops and a long horizontal stroke at the end.

Ian S. Piper
Compliance Officer
Premier Election Solutions, Inc.

CC: Trey Grayson (Kentucky Secretary of State)
 Dave Byrd (Premier President)
 Michael Lindroos (Premier Legal Counsel)
 Kathy Rogers (Premier Director of Gov't Affairs)
 Don Vopalensky (Premier State Certification Manager)



2007-01132

STATE BOARD OF ELECTIONS

Trey Grayson
Chairman
Secretary of State

140 Walnut Street
Frankfort, Kentucky 40601-3240
Phone: (502) 573-7100
Fax: (502) 573-4369
www.elect.ky.gov

Sarah Ball Johnson
Executive Director

Sandy Milburn
Assistant Director

August 30, 2007

The Honorable Greg Stumbo
Office of the Attorney General
Capitol Building, Suite 118
700 Capitol Avenue
Frankfort, Kentucky 40601-3449

Dear General Stumbo:

I have received your August 28, 2007 letter concerning the failure of Premier Elections Solutions, Inc. ("Premier", formerly known as Diebold Election Systems, Inc.) to properly provide Jefferson County with the 1.96.6 AccuVote Optical Scan software, as properly certified by the State Board of Elections on August 16, 2005.

The State Board of Elections provided your Assistant, Jennifer Black Hans, with copies of these certifications as well as Premier's August 27, 2007, correspondence explaining its mistake on August 28, 2007. You were forwarded the letter from Premier shortly after we received it and at our insistence. Any allegation that this information was reserved from your review by our office is wholly without merit.

Like you, we are disappointed that Premier mistakenly installed the wrong version of the software on the Jefferson County AccuVote optical scan ("OS") units. I applaud Premier's efforts to correct the mistake at no taxpayer expense in time for this fall's election, but it does not change the fact that a mistake was made and that such a mistake is unacceptable.

Your letter was obviously written before your staff had an opportunity to review these documents, or you would not have inappropriately accused the State Board of Elections of failing to certify the software used by Jefferson County. Indeed, all indications to the State Board of Elections were that Jefferson County's OS units were equipped with firmware version 1.96.6, the version certified for sale and use in Kentucky by the State Board of Elections on August 16, 2005. My August 7, 2007 letter to you was accurate to the best of my knowledge and to the information that had been relayed to our office in the past.

Letter to Hon. Greg Stumbo

August 30, 2007

Page 2 of 4

As you know, the General Assembly has placed the sole power and responsibility over the purchase and operation of Kentucky's voting systems in the hands of counties. In fact, you were a member of the General Assembly when the relevant statutes were adopted, and until late 2005, your Office represented the State Board. A cursory review of Kentucky election law provides that the fiscal court, or in this case metro government,

shall purchase or lease, from available funds or from the proceeds of bonds which may be issued for that purpose, voting machines, including extra or reserve machines, for use in regular, special and primary elections. The fiscal court may, prior to any election, authorize the use of additional voting machines in any particular precinct.

KRS 117.105. Furthermore, the county has further authority to

select in its discretion any type and make of voting machine that complies with the specifications and requirements of this chapter. The fiscal court may employ engineers and other skilled persons to advise and aid in the selection of the machines and in determining the specifications thereof.

KRS 117.115. Finally, the county maintains responsibility for the maintenance and upkeep of the voting machines on and in between Election Day:

When voting machines are acquired by any county, they shall be immediately placed in the custody of the county clerk, and shall remain in his custody at all times except when in use at an election or when in the custody of a court or court officer during contest proceedings. The clerk shall see that the machines are properly protected and preserved from damage or unnecessary deterioration, and shall not permit any unauthorized person to tamper with the machines.

KRS 117.135. Indeed, the counties maintain the sole responsibility for the selection, purchase, maintenance, and custody of voting systems. The State Board of Elections has no authority to dictate to the counties what voting systems they purchase, except to certify voting systems for use in the state of Kentucky, pursuant to KRS 117.379 and 117.381. **It is the county's responsibility to make sure that the system it purchases has been certified by the State Board of Elections and that the system that it contracts to purchase is what is actually received and installed in its county.**

As for the questions listed in your letter:

1. As previously stated, the State Board of Elections received the letter from Premier after the close of business on August 27, 2007, and at our insistence, it was emailed to your office on August 28, 2007. Our office also gave Ms. Hans access to the letter during her visit on August 28, 2007.
2. This question is addressed in Premier's letter to Jefferson County. Any further explanation should be given by Premier and Jefferson County.

3. The State Board of Elections will follow, as always, established election law enacted in KRS 117.379 and KRS 117.381 in the examination and certification of voting systems. The counties maintain responsibility for the selection, purchase and custody of such systems, pursuant to KRS 117.105, 117.115, and 117.135.
4. As stated in answer to question No. 1, your office was notified of the Premier letter at our insistence.
5. This question has been answered by the Premier letter. Any further inquiry will have to be answered by Premier and Jefferson County.
6. Jefferson County did not receive HAVA funds to purchase its OS units for its precincts. All Kentucky counties had access to federal funds as necessary to bring them into compliance with HAVA. Please see Kentucky's State Plan on our website at www.elect.ky.gov, which was approved by the State Board of Elections in 2003 under the able leadership of then Secretary of State and State Board of Elections Chairman John Y. Brown III. We have provided all necessary documentation of Kentucky's compliance with HAVA to the Election Assistance Commission.

I hope that this letter answers your questions about this matter. Should you have any additional questions, please contact us at your earliest convenience.

In closing, I must express my disappointment that this issue has devolved into a battle of headlines and press releases. We share the same goal – trying to improve Kentucky's elections. We disagree, however, about the best method of doing so.

At times, our offices have worked well together in trying to improve Kentucky's elections. One example in particular has been our work, along with the State Police, FBI and US Attorney's office, to address the vote fraud allegations in the 2006 primary elections in Bath County. In that instance, no press releases were issued; no accusatory letters were sent. Instead, all the relevant parties got together, shared the facts as they were known at the time, reviewed relevant law and divided up the work to bring vote buyers to justice. As a result of this cooperation, almost a dozen individuals have been indicted or convicted of vote buying in federal courts.

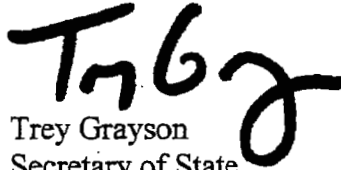
I hope that, as we go forward, the Bath County model is the one we follow. For example, perhaps we can develop proposed legislation for next year's General Assembly that provides for a steep financial penalty for voting system vendors that sell non-certified systems in Kentucky. California and Indiana both have such laws.

We can also identify other statutory and regulatory changes to give the State Board of Elections additional authority to better confirm the versions of the voting systems used in Kentucky counties.

Letter to Hon. Greg Stumbo
August 30, 2007
Page 4 of 4

If you are interested in discussing these or other areas of election law reform, I would be more than happy to meet with you. Working together, I am confident that we can continue to improve Kentucky elections.

Sincerely,

A handwritten signature in black ink, appearing to read 'Trey Grayson', written in a cursive style.

Trey Grayson
Secretary of State
Chairman, State Board of Elections
Commonwealth of Kentucky

cc: Mike Lindroos



2007-01141

STATE BOARD OF ELECTIONS

Trey Grayson
Chairman
Secretary of State

140 Walnut Street
Frankfort, Kentucky 40601-3240
Phone: (502) 573-7100
Fax: (502) 573-4369
www.elect.ky.gov

Sarah Ball Johnson
Executive Director

Sandy Milburn
Assistant Director

September 4, 2007

The Honorable Greg Stumbo
Office of the Attorney General
The Capitol, Suite 118
700 Capitol Avenue
Frankfort, Kentucky 40501-3449

Dear General Stumbo:

As stated in my August 21, 2007 correspondence, please allow this letter to inform you that the State Board of Elections' reexamination of the identified voting systems will take place on September 17 and 18, 2007, at the offices of the State Board of Elections at 140 Walnut Street, Frankfort, Kentucky 40601.

The examination by the examiners pursuant to KRS 117.379(2) will occur on Monday, September 17, 2007, at the following times (subject to the length of the presentations):

9:30 am-11:00 am	Election Systems & Software
12:30 pm-2:00 pm	Hart InterCivic
2:00 pm-3:30 pm	Premier Election Solutions (Formerly known as Diebold Election Systems)

The examination by the examiners is not subjected to the Open Meetings Act, as it is not a "meeting of a quorum of the members of any public agency." KRS 61.810(1). As a result, the examination by the examiners is not open to the public or the media. You and your staff are invited to the examination to only observe the examination in conjunction with your duties under KRS 15.243. However, we request that you and your staff do not interfere with the examiners in the exercise of their duties and refrain from engaging the examiners prior to and on examination day.

The examination by the State Board of Elections pursuant to KRS 117.379(2) will occur on Tuesday, September 18, 2007, at the following times (subject to the length of the presentations):

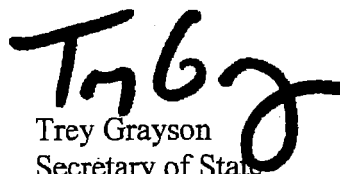
9:30 am-11:00 am Election Systems & Software
12:30 pm-2:00 pm Hart InterCivic
2:00 pm-3:30 pm Premier Election Solutions (Formerly known as Diebold Election Systems)

This meeting is open to the public and you are welcome to attend or send representatives from your staff to attend the examinations.

Please kindly provide us with notification of the number of representatives from your staff who will be attending the examinations so that we may accommodate your staff, as we have limited space at our facility.

Thank you for your cooperation in this matter. Please do not hesitate to contact us if you have any comments or questions.

Sincerely,

A handwritten signature in black ink, appearing to read 'Trey Grayson', written in a cursive style.

Trey Grayson
Secretary of State
Chairman, State Board of Elections
Commonwealth of Kentucky

ADDY-01107



Premier Election Solutions, Inc.
P.O. Box 1019
Allen, TX 75013
469 675-8990
fax 214 383-1586
www.premierelections.com

August 27, 2007

Attn: Susan Clark
Jefferson County Clerk's Office
P.O. Box 33033
Louisville, KY 40232-3033
Email: susanclark@jeffersoncountyclerk.org

VIA ELECTRONIC TRANSMISSION

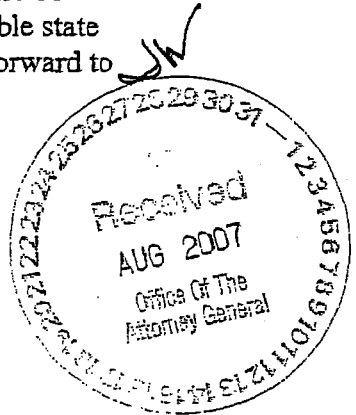
Re: Jefferson County, Kentucky AccuVote-OS Product Version

Dear Susan:

I am writing on behalf of Premier Election Solutions, Inc. (Premier) to make you aware that, within the last few days, a review of our records has revealed that the product version of the AccuVote-OS units deployed in Jefferson County, Kentucky are not a state certified version. The AccuVote-OS product version currently certified in the State of Kentucky is PC 1.96.6 with VSS 2002 compliant hardware. The AccuVote-OS units in use in Jefferson County are running firmware version PC 1.96.4 with hardware that was previously certified by the state but has not yet been upgraded to meet VSS 2002 compliance, which is now required by the State. This earlier version of firmware is, of course, fully federally certified and has been used extensively in several other states; nevertheless it does not have a certification in the State of Kentucky. We have informed the Kentucky Secretary of State's office of this matter.

We deeply regret this error. After an internal review, we have determined that our procedures for verifying state certified versions prior to shipping and implementation were not followed in detail in this case. With your approval, and the State's, Premier will implement a plan to immediately correct this error by upgrading your AccuVote-OS units, hardware and firmware, to the current state certified versions (as identified above) at no cost to the county.

I believe you will find that through Jefferson County's logic and accuracy testing and post-election auditing that there have been no functional or performance issues resulting from the use of the earlier versions of firmware and hardware. However, please be assured that Premier's policy is to provide systems that fully meet all applicable state certification requirements. Again, we apologize for this oversight and look forward to working with you to schedule an upgrade of your AccuVote-OS equipment.



If you have any questions, please contact me at on my cell phone (214.280.6464.)

Sincerely:

A handwritten signature in black ink, appearing to read 'Ian S. Piper', written over a horizontal line.

Ian S. Piper
Compliance Officer
Premier Election Solutions, Inc.

CC: Trey Grayson (Kentucky Secretary of State)
 Dave Byrd (Premier President)
 Michael Lindroos (Premier Legal Counsel)
 Kathy Rogers (Premier Director of Gov't Affairs)
 Don Vopalensky (Premier State Certification Manager)



COMMONWEALTH OF KENTUCKY
OFFICE OF THE ATTORNEY GENERAL

GREGORY D. STUMBO
ATTORNEY GENERAL

CAPITOL BUILDING, SUITE 118
700 CAPITOL AVENUE
FRANKFORT, KY 40601-3449
(502) 696-5300
FAX: (502) 564-2894

September 11, 2007

Via facsimile & hand-delivery

Secretary of State Trey Grayson
Chairman, State Board of Elections
Suite 152, State Capitol
700 Capitol Avenue
Frankfort, Kentucky 40601

RE: Investigation of Electronic Voting Systems

Dear Secretary Grayson:

In reply to your September 4, 2007 letter, I am pleased that the State Board of Elections ("SBE") is taking the necessary step of ordering a reexamination of electronic voting systems on September 17, 2007. I accept your September 4, 2007 invitation to observe this reexamination. OAG staff, including Assistant Attorneys General Jennifer Black Hans and Ryan Halloran, will be present at the reexamination on Monday, September 17, 2007. We are in the process of contracting with an independent, third-party consultant with experience in computer software and systems security, who will also be present as an agent of the OAG.

As requested, my staff will not interfere in any way with your examination process. Our goal is simply to ensure secure and reliable elections for Kentucky voters. In this regard, I do believe that the SBE's standardized checklist is woefully insufficient to truly test these voting systems. I agree with the League of Women Voters' call for independent computer experts who can ensure the accuracy and security of these voting systems. While an experienced information technology manager may be an excellent choice when deploying a new computer system, such experience is no substitute for a demonstrated expertise in software engineering and computer security.

At a minimum, the SBE's computer expert and the other examiners should have read the Source Code Team and Red Team reports, commissioned by the California Secretary of State and prepared by the University of California at Berkeley, and should be able to understand each of the reports in detail. These reports represent the most recent



Secretary Trey Grayson
Chair, State Board of Elections
RE: Investigation of Electronic Voting Systems
September 11, 2007
Page 2 of 3

top-to-bottom security analysis of the Hart InterCivic and Diebold systems currently in use in Kentucky. With regard to the reexamination of the Election Systems & Software (ES & S) iVotronic voting systems, the computer examiner should review *Software Review and Security Analysis of the ES&S iVotronic*, commissioned by the Florida Department of State and conducted by security experts at Florida State University. These reports are available at the respective web sites for the California and Florida Secretaries of State.

The examiners should also be prepared to ask specific questions to ensure the security, usability and accountability regarding each electronic voting system, including the following:

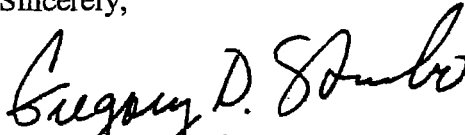
- ✓ Does the system include on its servers adequate security, which should include any necessary appliances, software or other protections that will guarantee no unauthorized access?
- ✓ For any voting devices or polling site components used in the system, can the vendor explain the necessity for each and every port or other means of access to the networked system? If not, why have the ports not been disabled?
- ✓ For any voting devices or polling site component used in the system, can the vendor explain the necessity for each modem or wireless connection? What is the potential for unauthorized access via these connections? Is there sufficient reason to recommend the disabling or banning of these connections?
- ✓ Does the deployment of the system in each purchasing county include the re-flashing, re-booting and/or re-installation of the firmware and/or software in all components of the voting system? Would the vendor be willing to provide this at no cost to the counties in order to ensure the accuracy of the system?
- ✓ Can the vendor identify the seals, the recommended chain-of-custody procedures and the security protocols for its system? How will these security procedures be communicated to the county clerks and poll workers?
- ✓ Can the vendor identify (name, manufacturer, model, version, etc.) the operating system and any third-party proprietary firmware or software components (including computer chips) used in its voting system? Will the vendor ensure and warrant the proper functioning of these third-party components in its system?
- ✓ Can the vendor identify what controls have been put in place since the 2006 elections to prevent (1) the switching of votes, (2) overvotes, (3) the failure to record votes, and (3) the tallying of shadow votes that would cause an inaccurate vote count?
- ✓ Can the vendor identify how precinct voting components will interface with vote tallying systems in place at the county clerk's office? Have interoperability concerns been adequately addressed since the 2006 elections?
- ✓ Can the vendor identify for each component of the system what specific controls are in place to report and reveal errors during any stage of the vote taking and tallying?

Secretary Trey Grayson
Chair, State Board of Elections
RE: Investigation of Electronic Voting Systems
September 11, 2007
Page 3 of 3

- ✓ If the vendor intends to offer components to provide a voter-verified paper audit trail or records, these components should be demonstrated in conjunction with the entire system, and not certified separately.

These recommendations are made in the spirit of cooperation, and it is my sincere hope that my continuing investigation of this matter will be met with the cooperation of the SBE and your office.

Sincerely,



Gregory D. Stumbo
Attorney General

Cc: Sarah Ball Johnson

TRANSMISSION VERIFICATION REPORT

TIME : 09/11/2007 12:05
NAME : ATTORNEY GENERAL
FAX : 5025642894
TEL :
SER.# : BROM4J184337

DATE, TIME	09/11 12:04
FAX NO./NAME	42476
DURATION	00:00:43
PAGE(S)	04
RESULT	OK
MODE	STANDARD ECM



COMMONWEALTH OF KENTUCKY
OFFICE OF THE ATTORNEY GENERAL

GREGORY D. STUMBO
ATTORNEY GENERAL

CAPITOL BUILDING, SUITE 118
700 CAPITOL AVENUE
FRANKFORT, KY 40601-3449
(502) 696-5300
FAX: (502) 564-2894

September 11, 2007

To: Secretary of State Trey Grayson

Company Name: Elections Branch

Telefax No.: (502) 564-2476

From: Gregory D. Stumbo

Division: Front

Total No. of Pages (including this page) 4

If you do not receive the total number of pages as shown above, please Contact:
Wendy Chandler at (502) 696-5614.

Comments:

TRANSMISSION VERIFICATION REPORT

TIME : 09/11/2007 11:54
NAME : ATTORNEY GENERAL
FAX : 5025642894
TEL :
SER. # : BROM4J184337

DATE, TIME	09/11 11:54
FAX NO./NAME	34369
DURATION	00:00:35
PAGE(S)	04
RESULT	OK
MODE	STANDARD ECM



COMMONWEALTH OF KENTUCKY
OFFICE OF THE ATTORNEY GENERAL

GREGORY D. STUMBO
ATTORNEY GENERAL

CAPITOL BUILDING, SUITE 118
700 CAPITOL AVENUE
FRANKFORT, KY 40601-3449
(502) 696-5300
FAX: (502) 564-2894

September 11, 2007

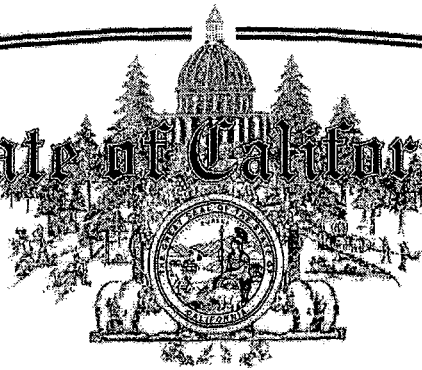
To: Sarah Ball Johnson
Company Name: State Board of Elections
Telefax No.: (502) 573-4369
From: Gregory D. Stumbo
Division: Front
Total No. of Pages (including this page) 4

If you do not receive the total number of pages as shown above, please Contact:
Wendy Chandler at (502) 696-5614.

Comments:

APPENDIX II

State of California



SECRETARY OF STATE

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

Whereas, pursuant to Elections Code section 19201, no voting system, in whole or in part, may be used unless it has received the approval of the Secretary of State; and

Whereas, Elections Code section 19222 requires that I, as Secretary of State for the State of California, conduct periodic reviews of voting systems to determine if they are defective, obsolete, or otherwise unacceptable; and

Whereas, at my inauguration as Secretary of State on January 8, 2007, I announced my intention to conduct a top-to-bottom review of voting systems approved for use in California; and

Whereas, on March 22, 2007, I circulated for public comment draft criteria for a review of voting systems approved for use in California, covering system security issues, access for voters with disabilities, access for minority language voters, and usability for elections officials and poll workers; and

Whereas, pursuant to my statutory obligations, I have undertaken such a review of voting systems approved for use in California, including the Hart Intercivic System 6.2.1 voting system, pursuant to a contract with the Regents of the University of California and conducted by experts selected and supervised by principal investigators from the computer science faculties of the Berkeley and Davis campuses, to determine if the voting systems are defective, obsolete, or otherwise unacceptable for use in the February 5, 2008, Presidential Primary Election and subsequent elections in California; and

Whereas, the study was completed on July 20, 2007, following which the expert reviewers delivered their written reports on their findings and methodology; and

Whereas, the expert reviewers found that the quality of the 2002 Voting System Standards (VSS) to which each of the three systems in their study were certified is inadequate, and noted

further that questions have been raised about the effectiveness of the testing; for example, Ciber, Inc., a testing laboratory involved in testing of voting systems under the 2002 VSS, has been denied interim accreditation for testing voting systems by the Federal Election Assistance Commission after finding that Ciber "was not following its quality-control procedures and could not document that it was conducting all the required tests"; and

Whereas, the expert reviewers demonstrated that the physical and technological security mechanisms provided by the vendors for each of the voting systems analyzed were inadequate to ensure accuracy and integrity of the election results and of the systems that provide those results; and

Whereas, the expert reviewers reported that all of the voting systems studied contain serious design flaws that have led directly to specific vulnerabilities, which attackers could exploit to affect election outcomes; and

Whereas, the Hart Source Code Review Team found that the Hart voting system contains design features that can be used in a fashion for which those design features were not intended, including network interfaces that are not secured against direct attack; and

Whereas, the Hart Source Code Review Team found that the Hart voting system's software fails to check the correctness of inputs from other Hart voting system components and uses those inputs in unsafe ways, potentially enabling an attacker to use voting system components to reprogram voting system units throughout the county with malicious code that would affect a subsequent election; and

Whereas, the Hart Source Code Review Team found that the Hart voting system exhibits a notable lack of the use of cryptographic security protocols to secure network communications, and where cryptography is used, a single countywide symmetric key is used that could allow a person to forge ballot information and election results in multiple polling locations; and

Whereas, the Hart Source Code Review Team found that the Hart voting system allows raw ballot records and other information to be used to reconstruct how each voter voted, potentially compromising the secrecy of the ballot; and

Whereas, the Hart Source Code Review Team found that many attacks are hard to detect and correct, defying development and implementation of simple, effective countermeasures; and

Whereas, the Hart Red Team that conducted penetration testing of the Hart voting system discovered multiple vulnerabilities; and

Whereas, on non-polling place components of the voting system that run on a Windows platform, Hart Red Team members located an undisclosed database user name and password and also manually bypassed Hart software security settings so they could run the Hart software in a standard Windows desktop environment, a possible vector for unauthorized access to the voting system's databases; and

Whereas, Hart Red Team members determined that the Hart voting system software fails to check the correctness of inputs from other Hart voting system components; and

Whereas, Hart Red Team members were able to access device-level menus on the Hart eScan precinct-based optical scan unit that should have been locked with passwords, which could allow access for altering voting system configuration settings; and

Whereas, Hart Red Team members confirmed findings from previous studies that allowed malicious actions to be performed on the Hart eScan precinct-based optical scan unit, including altering vote totals, using tools commonly found in an office; and

Whereas, Hart Red Team members were able to demonstrate the ability, after the close of the polls, to use a laptop computer to tamper with a Mobile Ballot Box memory device used to record votes cast on the eSlate direct decoding electronic voting device, an attack that, if undetected during the tampering, could alter vote totals in a manner not detected by technological safeguards but detectable in a manual recount; and

Whereas, Hart Red Team members found that the Hart voting system allows for remote eavesdropping and capture of the audio narration of a ballot (a feature designed for use by voters with disabilities), potentially violating the secrecy of the ballot; and

Whereas, architectural features of the Hart voting system significantly reduce its vulnerability to a viral attack introduced while the polls are open by a person with access only to the eSlate Direct Recording Electronic voting device; and

Whereas, architectural features of the Hart voting system significantly reduce its vulnerability to viral corruption of the voting system's central tally component through the introduction of malicious code at a polling place; and

Whereas, on July 30, 2007, a duly noticed public hearing was held to give interested persons an opportunity to express their views regarding the review of various voting systems, including the Hart Intercivic System 6.2.1 voting system; at this hearing, approximately 60 individuals testified; many more submitted comments by letter, facsimile transmission, and electronic mail; and

Whereas, pursuant to Elections Code section 19222, I, as Secretary of State, am authorized to withdraw approval previously granted of any voting system or part of a voting system if I determine that voting system or any part of that voting system to be defective or otherwise unacceptable; and

Whereas, I have reviewed the Hart Intercivic System 6.2.1 voting system and I have reviewed and considered several reports regarding the use of this voting system; the public testimony presented at the duly noticed public hearing held on July 30, 2007; and the comments submitted by letter, facsimile transmission, and electronic mail; and

Whereas, pursuant to Elections Code section 19222, six months' notice must be given before withdrawing approval previously granted of any voting system or part of a voting system unless I, as Secretary of State, for good cause shown, make a determination that a shorter period is necessary; and

Whereas, pursuant to Elections Code section 19222, any withdrawal by the Secretary of State of the previous approval of a voting system or part of a voting system is not effective as to any election conducted within six months of that withdrawal; now

Therefore, I, Debra Bowen, Secretary of State for the State of California, find and determine, pursuant to Division 19 of the Elections Code, as follows:

For the reasons set forth above, the Hart InterCivic System 6.2.1 voting system, comprised of JBC, version 4.3.1, eSlate/DAU, version 4.2.13, eScan, version 1.3.14, VBO, version 1.8.3, eCM Manager, version 1.1.7, Ballot Now software, version 3.3.11, BOSS software, version 4.3.13, Rally software, version 2.3.7, Tally software, version 4.3.10, and SERVO, version 4.2.10, which was previously approved, is found and determined to be defective or unacceptable and its certification and approval for use in subsequent elections in California is immediately withdrawn, except as specifically provided below.

1. Before any use in the February 5, 2008, Presidential primary election, jurisdictions must reinstall all software and firmware (including reformatting all hard disk drives and reinstalling the operating system where applicable) on all election management system servers and workstations, voting devices and hardware components of the voting system. Voting system application software must be reinstalled using the currently approved version obtained directly from the federal testing laboratory or the Secretary of State.
2. Within 30 days of the date of this document, the vendor must present a plan and uniform jurisdiction-use procedures to the Secretary of State for approval that will prevent future viral propagation of malicious software from one system component to another, such as from a voting system component located in one precinct to voting system components located in other precincts. The plan and use procedures must incorporate, or employ methods at least as effective as, a configuration of parallel central election management systems separated by an "air-gap" where (1) a permanent central system known to be running unaltered, certified software and firmware is used solely to define elections and program voting equipment and memory cards, (2) a physically-isolated duplicate system, reformatted after every election to guard against the possibility of infection, is used solely to read memory cards containing vote results, accumulate and tabulate those results and produce reports, and (3) a separate computer dedicated solely to this purpose is used to reformat all memory devices before they are connected to the permanent system again. (This "air-gap" model was proposed by the Source Code Review Team that reviewed the Diebold Election Systems, Inc., GEMS 1.18.24 voting system. Further details concerning the model are provided in Section 6.10 of the Source Code Review of the Diebold Voting System, dated July 20, 2007, and available on the Secretary of State

website at http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf.)

3. Within 30 days of the date of this document, the vendor must submit to the Secretary of State for approval specifications for the hardware and operating system platform that must be used for all applicable components of the voting system. The vendor must identify the requirements for "hardening" the configuration of that platform, including, but not limited to:
 - BIOS configuration;
 - Identification of essential services that are required and non-essential services that must be disabled;
 - Identification of essential ports that are required and non-essential ports that must be disabled and, if feasible, removed or physically blocked;
 - Audit logging configuration;
 - Definition of user security roles and associated permissions to assure all users have only the minimum required permissions for their role;
 - Password policies, including password strength, expiration, and maximum attempts, along with all related user account control settings; and
 - All utilities and software applications, with specifications for their installation, configuration and use, that are necessary for operation of the voting system (e.g., security software, data compression utilities, Adobe Acrobat, etc.).The vendor must identify automated mechanisms for jurisdictions to confirm and document that their system has been configured to these standards, and that all updatable components are the approved version and level. The vendor must provide full instructions for the use of these mechanisms, including expected results.
4. Immediately after any repair or modification of any voting system component, the integrity of the firmware and/or software must be verified using the automated mechanisms described above, or all software must be reinstalled by the jurisdiction from a read-only version of the approved firmware and/or software supplied directly by the federal testing laboratory or Secretary of State before the equipment can be put back into service.
5. Jurisdictions are prohibited from installing any software applications or utilities on any component of the voting system that have not been identified by the vendor and approved by the Secretary of State.
6. Within 30 days of the date of this document, the vendor must develop and submit to the Secretary of State for approval, a plan and procedures for timely identification of required security updates (e.g., operating system security patches, security software updates, etc.), vendor testing of the updates, and secure distribution and application of vendor-approved security updates.
7. Within 45 days of the date of this document, the vendor, working with jurisdiction users, must develop and submit to the Secretary of State for approval, uniform requirements and

use procedures for operating and maintaining the physical and logical security of the system, including, but not limited to:

- Physical security and access to the system and all components;
- Network security;
- Data security (including data backup requirements and procedures); and
- Separation of roles and responsibilities for jurisdiction personnel.

8. Network connections to any device not directly used and necessary for voting system functions are prohibited. Communication by or with any component of the voting system by wireless or modem transmission is prohibited at any time. No component of the voting system, or any device with network connectivity to the voting system, may be connected to the Internet, directly or indirectly, at any time.
9. Within 45 days of the date of this document, the vendor, working with jurisdiction users, must develop and submit to the Secretary of State for approval, detailed uniform requirements and use procedures for programming, pre- and post-election logic and accuracy testing, transporting and operating voting equipment that will prevent or detect unauthorized access to or modification of any component of the voting system, including, but not limited to:
 - Application of two-person rule;
 - Chain of custody controls and signature-verified documentation;
 - Requirements for secure interim storage of any system component; and
 - Employment of mechanisms to detect unauthorized access to the equipment.
10. Where tamper-evident seals are required to detect unauthorized access to a system component, those seals must be serialized and the vendor must specify in each instance the type of the seal to be used and the exact placement of that seal using photographs.
11. Upon request, members of the public must be permitted to observe and inspect, without physical contact, the integrity of all externally visible security seals used to secure voting equipment in a time and manner that does not interfere with the conduct of the election or the privacy of any voter.
12. Where voting equipment is used to record and tabulate vote results in a polling place, upon close of the polls, the poll workers are required to print two copies of the accumulated vote results and audit log from each JBC or eScan. Each poll worker must sign every copy. One copy of the vote results and audit log from each device must be publicly posted outside the polling place. The second copy must be included with the official election material that is returned to the jurisdiction headquarters on election night.
13. No poll worker or other person may record the time at which or the order in which voters vote in a polling place.
14. Poll workers are not permitted to have access to any VBO audit records, nor may they participate in any audits or recounts involving VBO audit records.

15. Within 60 days of the date of this document, the vendor, working with jurisdiction users, must develop and submit to the Secretary of State for approval, specific detailed uniform requirements and use procedures for vote results auditing and reconciliation, review of audit logs and retention of election documentation to validate vote results and detect unauthorized manipulation of vote results, including, but not limited to:
 - Precinct level ballot accounting;
 - Identification of abnormal voting patterns on VBO audit trails;
 - Escalation of audit sampling when significant discrepancies exist between electronic and manual audit vote results; and
 - Reconciliation of discrepancies between electronic and manual audit vote results.
16. Any post-election auditing requirements imposed as a condition of this certification shall be paid for by the vendor. Jurisdiction users are required to conduct the audits and the vendor is required to reimburse the jurisdiction.
17. After consultation with jurisdiction users, the Secretary of State shall establish additional post-election manual count auditing requirements, including:
 - Increased manual count sample sizes for close races, based on an adjustable sample model, where the size of the initial random sample depends on a number of factors, including the apparent margin of victory, the number of precincts, the number of ballots cast in each precinct, and a desired confidence level that the winner of the election has been called correctly. In establishing sampling requirements for close races, the Secretary of State may impose a specific sampling threshold for a given vote differential or percentage of the margin of victory, taking into account the number of electors and the number and size of precincts in the race.
 - Escalation requirements for expanding the manual count to additional precincts when discrepancies are found.
 - Uniform procedures to increase transparency and effectiveness of post-election manual count audits.
18. Each polling place must be equipped with a method or log in a format specified by the Secretary of State after consultation with the jurisdiction users to record all problems and issues with the voting equipment in the polling place as reported by voters or observed by poll workers. Such records must include the following information for each event:
 - Date and time of occurrence;
 - Voter involved, if any;
 - Equipment involved;
 - Brief description of occurrence;
 - Actions taken to resolve issue, if any; and
 - Election official(s) who observed and/or recorded the event.All such event logs or reports must be made available to the public for inspection and review upon request. Prior to or concurrent with the certification of the election, the jurisdiction election official must submit a report to the Secretary of State of all reported problems experienced with the voting system and identifying the actions taken, if any, to resolve the issues.

19. Training of poll workers must include the following:
- Secure storage of voting equipment while in the poll worker's possession;
 - Chain-of-custody procedures (including two person rule) required for voting equipment and polling place supplies;
 - Seal placement and procedures for verification of seal integrity;
 - Placement and observation of voting equipment;
 - Observation of activity that could indicate tampering or an attempt at tampering;
 - The Voter Bill of Rights set forth in section 2300 of the Elections Code;
 - The purpose served by the Voter Verified Paper Audit Trail (VVPAT), the importance of its use by voters, and how to handle problems such as paper jams;
 - A voter's right to vote on a paper ballot (in all DRE polling places) and how to handle requests for paper ballots;
 - The public right to inspect voting equipment and security seals, and how to handle requests for such inspections;
 - How to handle equipment failure or lack of sufficient paper ballots in a polling place and how to ensure continuity of the election in the event of such a failure; and
 - How to properly log all events and issues related to voting equipment in the polling place, including voter complaints of malfunctioning equipment.
20. All voters voting on paper ballots must be provided a privacy sleeve for their ballot and instructed on its use.
21. A warning must be posted in each voting booth stating that, pursuant to Elections Code sections 18564, 18565, 18566, 18567, 18568 and 18569, tampering with voting equipment or altering vote results constitutes a felony, punishable by imprisonment.
22. With respect to any piece of voting equipment for which the chain of custody has been compromised or for which the integrity of the tamper-evident seals has been compromised, the following actions must be taken:
- The chief election official of the jurisdiction must be notified immediately;
 - The equipment must be removed from service immediately and replaced if possible;
 - Any votes cast on the device prior to its removal from service must be subject to a 100% manual audit as part of the official canvass;
 - Any memory card containing data from that device must be secured and retained for the full election retention period;
 - An image of all device software and firmware must be stored on write-only media and retained securely for the full election retention period; and
 - All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing laboratory or the Secretary of State before the equipment is placed back into service.
23. If a voting device experiences a fatal error from which it cannot recover gracefully (i.e., the error is not handled through the device's internal error handling procedures with or without user input), such that the device must be rebooted or the device reboots itself to restore operation, the following actions must be taken:
- The chief election official of the jurisdiction must be notified immediately;

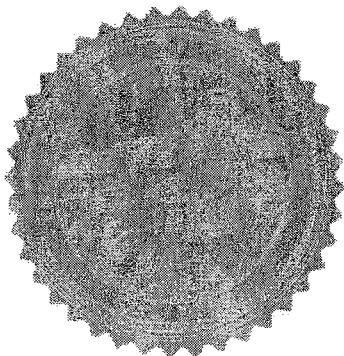
- The equipment must be removed from service immediately and replaced as soon as possible;
 - Any votes cast on the device prior to its removal from service must be subject to a 100% manual audit over and above the normal manual audit conducted during the official canvass;
 - Any memory card containing data from that device must be secured and retained for the full election retention period;
 - An image of all device software and firmware must be stored on write-only media and retained securely for the full election retention period;
 - The vendor shall provide an analysis of the cause of the failure;
 - Upon request by the Secretary of State, the vendor shall retain the device for a reasonable period of time to permit forensic analysis; and
 - All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing laboratory or the Secretary of State before the equipment is placed back into service.
24. The Secretary of State will review and finalize all plans, requirements and procedures submitted pursuant to the foregoing requirements above within thirty days of receipt. Upon approval, all such plans, requirements and procedures will automatically be incorporated into the official use procedures for the voting system, and will become binding upon all users of the system.
25. No substitution or modification of the voting system shall be made with respect to any component of the voting system, including the Use Procedures, until the Secretary of State has been notified in writing and has determined that the proposed change or modification does not impair the accuracy and efficiency of the voting system sufficient to require a re-examination and approval.
26. The Vendor developed utilities, Fusion, In-Fusion, Bravo and Trans, are specifically excluded from this certification.
27. The Secretary of State reserves the right, with reasonable notice to vendor and to the counties using the voting system, to modify the Use Procedures used with the voting system and to impose additional requirements with respect to the use of the system if the Secretary of State determines that such modifications or additions are necessary to enhance the accuracy, reliability or security of any of the voting system. Such modifications or additions shall be deemed to be incorporated herein as if set forth in full.
28. Any county using this voting system shall, prior to such use in each election, file with the California Secretary of State a copy of its Election Observer Panel plan.
29. The vendor agrees in writing to provide, and shall provide, to the Secretary of State, or to the Secretary of State's designee, within 30 days of the Secretary of State's demand for such, a working version of the voting system, including all hardware, firmware and software of the voting system, as well as the source code for any software or firmware contained in the voting system, including any commercial off the shelf software or firmware that is available and disclosable by the vendor, provided that the Secretary of

State first commits to the vendor in writing to maintain the confidentiality of the contents of such voting system or source code so as to protect the proprietary interests of the vendor in such voting system or source code. The terms of the commitment to maintain confidentiality shall be determined solely by the Secretary of State, after consultation with the vendor. The voting system shall not be installed in any California jurisdiction until the vendor has signed such an agreement. Any reasonable costs associated with the review of the source code for any software or firmware contained in the voting system shall be borne by the vendor.

30. The Secretary of State reserves the right to monitor activities before, during and after the election at any precinct or registrar of voters' office, and may, at his or her discretion, conduct a random parallel monitoring test of voting equipment.
31. By order of the Secretary of State, voting systems certified for use in California shall comply with all applicable state and federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002. Further, voting systems shall also comply with all state and federal voting system guidelines, standards, regulations and requirements that derive authority from or are promulgated pursuant to and in furtherance of the California Elections Code and the Help America Vote Act of 2002 or other applicable state or federal law when appropriate.
32. Voting system manufacturers or their agents shall assume full responsibility for any representation they make that a voting system complies with all applicable state and federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002. In the event such representation is determined to be false or misleading, voting system manufacturers or their agents shall be responsible for the cost of any upgrade, retrofit or replacement of any voting system or its component parts found to be necessary for certification or otherwise not in compliance.
33. Any voting system purchased with funds allocated by the Secretary of State's office shall meet all applicable state and federal standards, regulations and requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002.
34. The vendor must establish a California County User Group and hold at least one annual meeting where all California users and Secretary of State staff are invited to attend and review the system and ensure voter accessibility.
35. In addition to depositing the source code in an approved escrow facility, the vendor must deposit with the Secretary of State a copy of the system source code, binary executables and tools and documentation, to allow the complete and successful compilation and installation of a system in its production/operational environment with confirmation by a

verification test by qualified personnel using only this content. The Secretary of State reserves the right to perform a full independent review of the source code at any time.

36. The vendor must provide printing specifications for paper ballots to the Secretary of State. The Secretary of State will certify printers to print ballots for this system based upon their demonstrated ability to do so. The vendor may not require exclusivity in ballot printing and must cooperate fully in certification testing of ballots produced by other ballot printers.

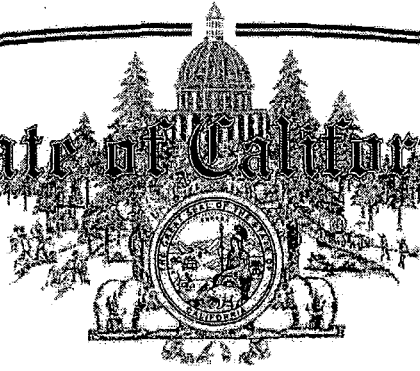


IN WITNESS WHEREOF, I hereunto set my hand and affix the Great Seal of the State of California, this 3rd day of August, 2007.

Handwritten signature of Debra Bowen in cursive script.

DEBRA BOWEN
Secretary of State

State of California



SECRETARY OF STATE

WITHDRAWAL OF APPROVAL OF DIEBOLD ELECTION SYSTEMS, INC., GEMS 1.18.24/AccuVote-TSX/AccuVote-OS DRE & OPTICAL SCAN VOTING SYSTEM AND CONDITIONAL RE-APPROVAL OF USE OF DIEBOLD ELECTION SYSTEMS, INC., GEMS 1.18.24/AccuVote-TSX/AccuVote-OS DRE & OPTICAL SCAN VOTING SYSTEM

Whereas, pursuant to Elections Code section 19201, no voting system, in whole or in part, may be used unless it has received the approval of the Secretary of State; and

Whereas, Elections Code section 19222 requires that I, as Secretary of State for the State of California, conduct periodic reviews of voting systems to determine if they are defective, obsolete, or otherwise unacceptable; and

Whereas, at my inauguration as Secretary of State on January 8, 2007, I announced my intention to conduct a top-to-bottom review of voting systems approved for use in California; and

Whereas, on March 22, 2007, I circulated for public comment draft criteria for a review of voting systems approved for use in California, covering system security issues, access for voters with disabilities, access for minority language voters, and usability for elections officials and poll workers; and

Whereas, pursuant to my statutory obligations, I have undertaken such a review of voting systems approved for use in California, including the Diebold Election Systems, Inc., GEMS 1.18.24/AccuVote-TSX/AccuVote-OS voting system, pursuant to a contract with the Regents of the University of California and conducted by experts selected and supervised by principal investigators from the computer science faculties of the Berkeley and Davis campuses, to determine if the voting systems are defective, obsolete, or otherwise unacceptable for use in the February 5, 2008, Presidential Primary Election and subsequent elections in California; and

Whereas, the study was completed on July 20, 2007, following which the expert reviewers delivered their written reports on their findings and methodology; and

Whereas, the expert reviewers found that the quality of the 2002 Voting System Standards (VSS) to which each of the three systems in their study were certified is inadequate, and noted further that questions have been raised about the effectiveness of the testing; for example, Ciber, Inc., a testing laboratory involved in testing of voting systems under the 2002 VSS, has been denied interim accreditation for testing voting systems by the Federal Election Assistance Commission after finding that Ciber “was not following its quality-control procedures and could not document that it was conducting all the required tests”; and

Whereas, the expert reviewers demonstrated that the physical and technological security mechanisms provided by the vendors for each of the voting systems analyzed were inadequate to ensure accuracy and integrity of the election results and of the systems that provide those results; and

Whereas, the expert reviewers reported that all of the voting systems studied contain serious design flaws that have led directly to specific vulnerabilities, which attackers could exploit to affect election outcomes; and

Whereas, the Diebold Source Code Review Team found that the Diebold software contains vulnerabilities that could allow an attacker to install malicious software on voting machines and on the election management system, which could cause votes to be recorded incorrectly or to be miscounted, possibly altering election results; and

Whereas, the Diebold Source Code Review Team found that the Diebold system is susceptible to computer viruses that propagate from voting machine to voting machine and even voting machines to the election management system, which could allow an attacker with access to only one voting unit or memory card to spread malicious code, between elections, to many, if not all, of a county’s voting units; and

Whereas, the Diebold Source Code Review Team found that due to these shortcomings some threats would be difficult, if not impossible, to remedy with election procedures; and

Whereas, the Diebold Source Code Review Team found that both the electronic and paper records of the Diebold TSx direct recording electronic voting machine contain enough information to compromise the secrecy of the ballot; and

Whereas, the Diebold Red Team that conducted penetration testing on the Diebold voting system performed vulnerability scans of the Diebold voting system and discovered multiple vulnerabilities; and

Whereas, the Diebold Red Team members, with access only to the Windows operating system on the Diebold GEMS election management server supplied by Diebold and without requiring access to Diebold source code were able to access the Diebold voting system server software and to corrupt the election management system database, which could result in manipulated voter totals or the inability to read election results, rendering an election impossible to complete electronically; and

Whereas, without requiring access to Diebold source code, the Diebold Red Team members gained “root access” to the voting system that allowed manipulation of every setting on the networking devices and on the election management system server; and

Whereas, the Diebold Red Team members, without accessing Diebold source code, were able to violate the physical security of every aspect of the TSx direct recording electronic voting machine under polling place conditions using tools found in a typical office; and

Whereas, the Diebold Red Team members identified attacks on the TSx direct recording electronic voting machine that could allow a voter to delete all electronic records of ballots cast up to the time of the attack, including backup records; and

Whereas, the Diebold Red Team found a simple attack that can put the AVPM voter verifiable paper audit trail (VVPAT) printer out of service until the TSx unit is rebooted, using only tools that can be found in a typical office, in which voters who were not aware that they should expect a printed version of their ballot for review would not observe anything unusual, because the attack also causes the TSx to stop issuing reminders to voters that they should verify the printed record of their selections; and

Whereas, the Diebold Red Team members also found that the design of the AVPM VVPAT printer enabled attacks on the printed records of voter’s ballots using a common household substance that could covertly destroy the VVPAT records, particularly notable because the attack (1) affects records printed before the attack is executed, (2) affects records printed after the attack is executed, (3) does not affect the way records are displayed to voters as they are produced – so as to avoid raising voter suspicion before the close of polls, (4) does not affect the printer mechanisms or jam the printer – again, to avoid raising suspicion, (5) the impact of these attacks is to make many of the VVPAT-printed records completely unreadable and most of them barely or only partially readable, destroying records already printed by the VVPAT at the time of the attack and potentially destroying all records produced throughout the rest of the day by that particular VVPAT, and (6) the attack is particularly viable on the TSx because the design of the VVPAT printer and the security casing for printed records allows the attack substance to linger undetected inside the machine until the end of election day; neither subsequent voters nor poll workers would know the attack had taken place until the printed records were removed at the end of Election Day; and

Whereas, the impact (once discovered) of the household substance attack on the VVPAT is highly visible, but when combined with an electronic attack that destroyed ballots, it could serve to effectively nullify most – if not all – of the votes cast on a particular TSx unit; and

Whereas, the Diebold Red Team members, without accessing Diebold source code, gained access to the election management server to manipulate and corrupt the election management system database; and

Whereas, some of these attacks could be carried out in a manner that is not subject to detection by audit, including review of software logs; and

Whereas, intellectual property is in any event notoriously difficult to protect against theft or unauthorized access, voting system source code being no less vulnerable; and

Whereas, Diebold left source code for one of its direct recording electronic voting machines unprotected on the Internet, from which it was downloaded and subsequently examined by many people, including computer security experts and other computer scientists; and

Whereas, a Diebold direct recording electronic voting machine was offered for sale on eBay, the Internet auction site; and

Whereas, tampering with optical scan equipment such as the Diebold AccuVote-OS precinct scanner and the AccuVote-OS Central Count can be readily detected and corrected through hand counting of the optical scan paper ballots marked and directly verified by voters; and

Whereas, voted and unvoted optical scan paper ballots can be secured through well-developed and tested physical security policies and procedures; and

Whereas, tampering with direct recording electronic voting machines such as the TSx can be difficult or impossible to detect, and is also difficult or impossible to correct through hand counting of VVPAT records, particularly when combined with successful attacks on VVPAT printing systems such as the AccuView Printer Module used with the TSx; and

Whereas, studies have shown that many voters do not review VVPAT records and that test voters who do review VVPAT records do not detect many discrepancies that have been intentionally introduced between selections shown on the paper record and selections shown on the review screen of a direct recording electronic voting machine; and

Whereas, on July 30, 2007, a duly noticed public hearing was held to give interested persons an opportunity to express their views regarding the review of various voting systems, including the Diebold Election Systems, Inc., GEMS 1.18.24/AccuVote-TSX/AccuVote-OS voting system. At this hearing, approximately 60 individuals testified. Many more submitted comments by letter, facsimile transmission, and electronic mail; and

Whereas, pursuant to Elections Code section 19222, I, as Secretary of State, am authorized to withdraw approval previously granted of any voting system or part of a voting system if I determine that voting system or any part of that voting system to be defective or otherwise unacceptable; and

Whereas, I have reviewed the Diebold GEMS 1.18.24/AccuVote-TSX/AccuVote-OS voting system and I have reviewed and considered several reports regarding the use of this voting system; the public testimony presented at the duly noticed public hearing held on July 30, 2007; and the comments submitted by letter, facsimile transmission, and electronic mail; and

Whereas, pursuant to Elections Code section 19222, six months' notice must be given before withdrawing approval previously granted of any voting system or part of a voting system unless

I, as Secretary of State, for good cause shown, make a determination that a shorter period is necessary; and

Whereas, pursuant to Elections Code section 19222, any withdrawal by the Secretary of State of the previous approval of a voting system or part of a voting system is not effective as to any election conducted within six months of that withdrawal; now

Therefore, I, Debra Bowen, Secretary of State for the State of California, find and determine, pursuant to Division 19 of the Elections Code, as follows:

For the reasons set forth above, the Diebold Elections Systems, Inc., voting system, comprised of GEMS software, version 1.18.24, AccuVote-TSX with AccuView Printer Module and Ballot Station firmware version 4.6.4, AccuVote-OS (Model D) with firmware version 1.96.6, AccuVote-OS Central Count with firmware version 2.0.12, AccuFeed, Vote Card Encoder, version 1.3.2, Key Card Tool software, version 4.6.1, and VC Programmer software, version 4.6.1, which was previously approved, is found and determined to be defective or unacceptable and its certification and approval for use in subsequent elections in California is immediately withdrawn, except as specifically provided below.

1. In order to provide accessible balloting to voters with disabilities in compliance with HAVA, jurisdictions may use no more than one AccuVote-TSx per polling place on Election Day. To protect voter privacy, jurisdictions are required to ensure that at least five persons voluntarily cast their ballot on each such device over the course of Election Day.
2. The AccuVote-TSx may be used in early voting prior to Election Day, subject to the following restrictions:
 - After the close of the polls each day of early voting, all voting equipment must be secured against tampering and returned by jurisdiction elections employees for storage in a jurisdiction facility that meets the security standards that apply to the jurisdiction's election headquarters;
 - Early voting centers may only be staffed by jurisdiction elections employees;
 - The jurisdiction must staff the early voting so that one employee is responsible solely for monitoring the voting equipment to ensure no unauthorized access to the equipment occurs;
 - The jurisdiction must maintain a chain of custody log for each piece of equipment, in which two or more jurisdiction employees record, verify and sign off on the public counter numbers on the device, the integrity of the tamper-evident-seals and the serial number of those seals at the opening and closing of the polls each day of early voting; and
 - The jurisdiction must conduct a 100% manual count of all votes cast on an AccuVote-TSx.
3. The elections official must reset the encryption key used for all AccuVote-TSx units to change the key from the factory default setting to a unique value for each election prior to programming any units.

4. Before any use in the February 5, 2008, Presidential primary election, jurisdictions must reinstall all software and firmware (including reformatting all hard disk drives and reinstalling the operating system where applicable) on all election management system servers and workstations, voting devices and hardware components of the voting system. Voting system application software must be reinstalled using the currently approved version obtained directly from the federal testing laboratory or the Secretary of State.
5. Within 30 days of the date of this document, the vendor must present a plan and uniform jurisdiction-use procedures to the Secretary of State for approval that will prevent future viral propagation of malicious software from one system component to another, such as from a voting system component located in one precinct to voting system components located in other precincts. The plan and use procedures must incorporate, or employ methods at least as effective as, a configuration of parallel central election management systems separated by an "air-gap" where (1) a permanent central system known to be running unaltered, certified software and firmware is used solely to define elections and program voting equipment and memory cards, (2) a physically-isolated duplicate system, reformatted after every election to guard against the possibility of infection, is used solely to read memory cards containing vote results, accumulate and tabulate those results and produce reports, and (3) a separate computer dedicated solely to this purpose is used to reformat all memory devices before they are connected to the permanent system again. (This "air-gap" model was proposed by the Source Code Review Team that reviewed the Diebold Election Systems, Inc., GEMS 1.18.24 voting system. Further details concerning the model are provided in Section 6.10 of the Source Code Review of the Diebold Voting System, dated July 20, 2007, and available on the Secretary of State website at http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf.)
6. Within 30 days of the date of this document, the vendor must submit to the Secretary of State for approval specifications for the hardware and operating system platform that must be used for all applicable components of the voting system. The vendor must identify the requirements for "hardening" the configuration of that platform, including, but not limited to:
 - BIOS configuration;
 - Identification of essential services that are required and non-essential services that must be disabled;
 - Identification of essential ports that are required and non-essential ports that must be disabled and, if feasible, removed or physically blocked;
 - Audit logging configuration;
 - Definition of user security roles and associated permissions to assure all users have only the minimum required permissions for their role;
 - Password policies, including password strength, expiration, and maximum attempts, along with all related user account control settings; and
 - All utilities and software applications, with specifications for their installation, configuration and use, that are necessary for operation of the voting system (e.g., security software, data compression utilities, Adobe Acrobat, etc.).

The vendor must identify automated mechanisms for jurisdictions to confirm and document that their system has been configured to these standards, and that all updatable components are the approved version and level. The vendor must provide full instructions for the use of these mechanisms, including expected results.

7. Immediately after any repair or modification of any voting system component, the integrity of the firmware and/or software must be verified using the automated mechanisms described above, or all software must be reinstalled by the jurisdiction from a read-only version of the approved firmware and/or software supplied directly by the federal testing laboratory or Secretary of State before the equipment can be put back into service.
8. Jurisdictions are prohibited from installing any software applications or utilities on any component of the voting system that have not been identified by the vendor and approved by the Secretary of State.
9. Within 30 days of the date of this document, the vendor must develop and submit to the Secretary of State for approval, a plan and procedures for timely identification of required security updates (e.g., operating system security patches, security software updates, etc), vendor testing of the updates, and secure distribution and application of vendor-approved security updates.
10. Within 45 days of the date of this document, the vendor, working with jurisdiction users, must develop and submit to the Secretary of State for approval, uniform requirements and use procedures for operating and maintaining the physical and logical security of the system, including, but not limited to:
 - Physical security and access to the system and all components;
 - Network security;
 - Data security (including data backup requirements and procedures); and
 - Separation of roles and responsibilities for jurisdiction personnel.
11. Network connections to any device not directly used and necessary for voting system functions are prohibited. Communication by or with any component of the voting system by wireless or modem transmission is prohibited at any time. No component of the voting system, or any device with network connectivity to the voting system, may be connected to the Internet, directly or indirectly, at any time.
12. Within 45 days of the date of this document, the vendor, working with jurisdiction users, must develop and submit to the Secretary of State for approval, detailed uniform requirements and use procedures for programming, pre- and post-election logic and accuracy testing, transporting and operating voting equipment that will prevent or detect unauthorized access to or modification of any component of the voting system, including, but not limited to:
 - Application of two-person rule;
 - Chain of custody controls and signature-verified documentation;
 - Requirements for secure interim storage of any system component; and
 - Employment of mechanisms to detect unauthorized access to the equipment.

13. Where tamper-evident seals are required to detect unauthorized access to a system component, those seals must be serialized and the vendor must specify in each instance the type of the seal to be used and the exact placement of that seal using photographs.
14. Upon request, members of the public must be permitted to observe and inspect, without physical contact, the integrity of all externally visible security seals used to secure voting equipment in a time and manner that does not interfere with the conduct of the election or the privacy of any voter.
15. Where voting equipment is used to record and tabulate vote results in a polling place, upon close of the polls, the poll workers are required to print two copies of the accumulated vote results and audit log from each device. Each poll worker must sign every copy. One copy of the vote results and audit log from each device must be publicly posted outside the polling place. The second copy must be included with the official election material that is returned to the jurisdiction headquarters on election night.
16. No poll worker or other person may record the time at which or the order in which voters vote in a polling place.
17. Poll workers are not permitted to have access to any AVPM audit records, nor may they participate in any audits or recounts involving AVPM audit records.
18. Within 60 days of the date of this document, the vendor, working with jurisdiction users, must develop and submit to the Secretary of State for approval, specific detailed uniform requirements and use procedures for vote results auditing and reconciliation, review of audit logs and retention of election documentation to validate vote results and detect unauthorized manipulation of vote results, including, but not limited to:
 - Precinct level ballot accounting;
 - Identification of abnormal voting patterns on AVPM audit trails;
 - Escalation of audit sampling when significant discrepancies exist between electronic and manual audit vote results; and
 - Reconciliation of discrepancies between electronic and manual audit vote results.
19. Any post-election auditing requirements imposed as a condition of this certification shall be paid for by the vendor. Jurisdiction users are required to conduct the audits and the vendor is required to reimburse the jurisdiction.
20. After consultation with jurisdiction users, the Secretary of State shall establish additional post-election manual count auditing requirements, including:
 - Increased manual count sample sizes for close races, based on an adjustable sample model, where the size of the initial random sample depends on a number of factors, including the apparent margin of victory, the number of precincts, the number of ballots cast in each precinct, and a desired confidence level that the winner of the election has been called correctly. In establishing sampling requirements for close races, the Secretary of State may impose a specific sampling threshold for a given vote differential or percentage of the margin of victory, taking into account the number of electors and the number and size of precincts in the race;

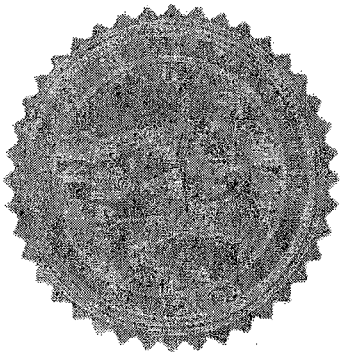
- Escalation requirements for expanding the manual count to additional precincts when discrepancies are found; and
 - Uniform procedures to increase transparency and effectiveness of post-election manual count audits.
21. User jurisdictions are required to conduct a 100% manual count audit of the electronic results tabulated on each DRE machine in use on Election Day.
22. Each polling place must be equipped with a method or log in a format specified by the Secretary of State after consultation with the jurisdiction users to record all problems and issues with the voting equipment in the polling place as reported by voters or observed by poll workers. Such records must include the following information for each event:
- Date and time of occurrence;
 - Voter involved, if any;
 - Equipment involved;
 - Brief description of occurrence;
 - Actions taken to resolve issue, if any; and
 - Election official(s) who observed and/or recorded the event.
23. All such event logs or reports must be made available to the public for inspection and review upon request. Prior to or concurrent with the certification of the election, the jurisdiction election official must submit a report to the Secretary of State of all reported problems experienced with the voting system and identifying the actions taken, if any, to resolve the issues.
24. Training of poll workers must include the following:
- Secure storage of voting equipment while in the poll worker's possession;
 - Chain-of-custody procedures (including two person rule) required for voting equipment and polling place supplies;
 - Seal placement and procedures for verification of seal integrity;
 - Placement and observation of voting equipment;
 - Observation of activity that could indicate tampering or an attempt at tampering;
 - The Voter Bill of Rights set forth in section 2300 of the Elections Code;
 - The purpose served by the Voter Verified Paper Audit Trail (VVPAT), the importance of its use by voters, and how to handle problems such as paper jams;
 - How to ensure that a minimum of five voters vote on each DRE in a polling place;
 - The public right to inspect voting equipment and security seals, and how to handle requests for such inspection;
 - How to handle equipment failure or lack of sufficient paper ballots in a polling place and how to ensure continuity of the election in the event of such a failure; and
 - How to properly log all events and issues related to voting equipment in the polling place, including voter complaints of malfunctioning equipment.
25. All voters voting on paper ballots must be provided a privacy sleeve for their ballot and instructed on its use.

26. A warning must be posted in each voting booth stating that, pursuant to Elections Code sections 18564, 18565, 18566, 18567, 18568 and 18569, tampering with voting equipment or altering vote results constitutes a felony, punishable by imprisonment.
27. With respect to any piece of voting equipment for which the chain of custody has been compromised or for which the integrity of the tamper-evident seals has been compromised, the following actions must be taken:
- The chief election official of the jurisdiction must be notified immediately;
 - The equipment must be removed from service immediately and replaced if possible;
 - Any votes cast on the device prior to its removal from service must be subject to a 100% manual audit as part of the official canvass;
 - Any memory card containing data from that device must be secured and retained for the full election retention period;
 - An image of all device software and firmware must be stored on write-only media and retained securely for the full election retention period; and
 - All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing laboratory or the Secretary of State before the equipment is placed back into service.
28. If a voting device experiences a fatal error from which it cannot recover gracefully (i.e., the error is not handled through the device's internal error handling procedures with or without user input), such that the device must be rebooted or the device reboots itself to restore operation, the following actions must be taken:
- The chief election official of the jurisdiction must be notified immediately;
 - The equipment must be removed from service immediately and replaced as soon as possible;
 - Any votes cast on the device prior to its removal from service must be subject to a 100% manual audit over and above the normal manual audit conducted during the official canvass;
 - Any memory card containing data from that device must be secured and retained for the full election retention period;
 - An image of all device software and firmware must be stored on write-only media and retained securely for the full election retention period;
 - The vendor shall provide an analysis of the cause of the failure;
 - Upon request by the Secretary of State, the vendor shall retain the device for a reasonable period of time to permit forensic analysis; and
 - All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing laboratory or the Secretary of State before the equipment is placed back into service.
29. The Secretary of State will review and finalize all plans, requirements and procedures submitted pursuant to the foregoing requirements above within thirty days of receipt. Upon approval, all such plans, requirements and procedures will automatically be incorporated into the official use procedures for the voting system, and will become binding upon all users of the system.

30. No substitution or modification of the voting system shall be made with respect to any component of the voting system, including the Use Procedures, until the Secretary of State has been notified in writing and has determined that the proposed change or modification does not impair the accuracy and efficiency of the voting system sufficient to require a re-examination and approval.
31. The Secretary of State reserves the right, with reasonable notice to vendor and to the counties using the voting system, to modify the Use Procedures used with the voting system and to impose additional requirements with respect to the use of the system if the Secretary of State determines that such modifications or additions are necessary to enhance the accuracy, reliability or security of any of the voting system. Such modifications or additions shall be deemed to be incorporated herein as if set forth in full.
32. Any county using this voting system shall, prior to such use in each election, file with the California Secretary of State a copy of its Election Observer Panel plan.
33. The vendor agrees in writing to provide, and shall provide, to the Secretary of State, or to the Secretary of State's designee, within 30 days of the Secretary of State's demand for such, a working version of the voting system, including all hardware, firmware and software of the voting system, as well as the source code for any software or firmware contained in the voting system, including any commercial off the shelf software or firmware that is available and disclosable by the vendor, provided that the Secretary of State first commits to the vendor in writing to maintain the confidentiality of the contents of such voting system or source code so as to protect the proprietary interests of the vendor in such voting system or source code. The terms of the commitment to maintain confidentiality shall be determined solely by the Secretary of State, after consultation with the vendor. The voting system shall not be installed in any California jurisdiction until the vendor has signed such an agreement. Any reasonable costs associated with the review of the source code for any software or firmware contained in the voting system shall be born by the vendor.
34. The Secretary of State reserves the right to monitor activities before, during and after the election at any precinct or registrar of voters' office, and may, at his or her discretion, conduct a random parallel monitoring test of voting equipment.
35. By order of the Secretary of State, voting systems certified for use in California shall comply with all applicable state and federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002. Further, voting systems shall also comply with all state and federal voting system guidelines, standards, regulations and requirements that derive authority from or are promulgated pursuant to and in furtherance of California Elections Code and the Help America Vote Act of 2002 or other applicable state or federal law when appropriate.
36. Voting system manufacturers or their agents shall assume full responsibility for any representation they make that a voting system complies with all applicable state and

federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002. In the event such representation is determined to be false or misleading, voting system manufacturers or their agents shall be responsible for the cost of any upgrade, retrofit or replacement of any voting system or its component parts found to be necessary for certification or otherwise not in compliance.

37. Any voting system purchased with funds allocated by the Secretary of State's office shall meet all applicable state and federal standards, regulations and requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002.
38. The vendor must establish a California County User Group and hold at least one annual meeting where all California users and Secretary of State staff are invited to attend and review the system and ensure voter accessibility.
39. In addition to depositing the source code in an approved escrow facility, the vendor must deposit with the Secretary of State a copy of the system source code, binary executables and tools and documentation, to allow the complete and successful compilation and installation of a system in its production/operational environment with confirmation by a verification test by qualified personnel using only this content. The Secretary of State reserves the right to perform a full independent review of the source code at any time.
40. The vendor must provide printing specifications for paper ballots to the Secretary of State. The Secretary of State will certify printers to print ballots for this system based upon their demonstrated ability to do so. The vendor may not require exclusivity in ballot printing and must cooperate fully in certification testing of ballots produced by other ballot printers.



IN WITNESS WHEREOF, I hereunto set my hand and affix the Great Seal of the State of California, this 3rd day of August, 2007.

DEBRA BOWEN
Secretary of State

APPENDIX III



Newsweek

Levy: Electronic Voting Machines Aren't Ready for '08

By Steven Levy
Newsweek

Sept. 10, 2007 issue - Next year we'll have the second presidential election since the horribly botched one in 2000. Can we expect better? An answer comes from the highest election official in the most populated state in the Union. Worried about a string of reported vulnerabilities, Debra Bowen, California's secretary of State, had asked computer scientists at the University of California to conduct a "top to bottom" analysis of the thousands of touchscreen electronic voting machines in use in the Golden State. Next year millions of voters will use these systems, manufactured by the industry's largest suppliers, not only in California but in many other states as well.

What did the study reveal? "Things were worse than I thought," says Bowen. "There were far too many ways that people with ill intentions could compromise the voting systems without detection." Some of those security holes could, in theory, allow a dirty trickster with access to a single machine to infiltrate the central vote-counting system and covertly toss an election to the wrong candidate.

It was the most devastating confirmation to date of what security experts have been saying for years: vulnerabilities in election machines are so severe that voters have no way of knowing for sure that the choices they enter into the touchscreens and ballots will actually be counted. "The studies show that these machines are basically poison," says Avi Rubin, a Johns Hopkins computer-science professor and voting-security expert.

Bowen's response, on Aug. 3, was to take the extreme step of decertifying the voting machines (this to the dismay of those defending the touchscreen vendors, who claimed that the tests did not reflect real-world conditions). Because California voters do need something to vote on, though, she allowed the use of some, mandating a rigorous set of controls (like "hardening" the security protocols) to make sure that the flaws aren't exploited. Now it's up to those in charge of elections in other states to step up and take similar measures for 2008.

One desperately needed measure is a national law to implement what is known as a voting paper trail—the ballot equivalent of a receipt in a cash register. (Voters get to look at a printout of their voting choices and leave the paper behind for recounts and audits.) A "voting integrity" bill introduced by Rep. Rush Holt, a New Jersey Democrat, would do just that—if it ever passes. "We just didn't get it to the floor before the August recess," says Holt, who is hoping for what seems like a long shot—that the bill will be quickly voted on, a similar bill in the Senate will also get the hurry-up treatment and that the president will sign it. (The GOP has generally been less active in pushing for this type of reform.) "It's still possible [to get it done in time for '08], but each day it gets a little less possible," he says.

The paper trail is no panacea: the California study shows that even that system can be hacked. And some reformers claim that the Holt bill doesn't go far enough. But Holt insists that a national law is the only solution. "If you leave it to the states, some won't do it," he says.

It's reasonable to ask why the same wizards who can come up with ATMs, predator drones and Google can't produce secure, verifiable ballots. Eventually they will, if we encourage innovation, transparency and accountability in the ballot industry. But we're electing a new president next year, and it's so late in the game that the only measures to stop another mistrusted election are stopgaps. California's secretary of State recognizes that. Plenty of citizens get it, too. Why aren't more elected officials standing up for our elections?

URL: <http://www.msnbc.msn.com/id/20546322/site/newsweek/>

MSN Privacy . Legal
© 2007 MSNBC.com

APPENDIX IV



Premier Election Solutions, Inc.
P.O. Box 1019
Allen, TX 75013
469 675-8990
fax 214 383-1596
www.premierelections.com

August 27, 2007

Attn: Susan Clark
Jefferson County Clerk's Office
P.O. Box 33033
Louisville, KY 40232-3033
Email: susanclark@jeffersoncountyclerk.org

VIA ELECTRONIC TRANSMISSION

Re: Jefferson County, Kentucky AccuVote-OS Product Version

Dear Susan:

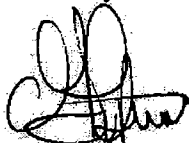
I am writing on behalf of Premier Election Solutions, Inc. (Premier) to make you aware that, within the last few days, a review of our records has revealed that the product version of the AccuVote-OS units deployed in Jefferson County, Kentucky are not a state certified version. The AccuVote-OS product version currently certified in the State of Kentucky is PC 1.96.6 with VSS 2002 compliant hardware. The AccuVote-OS units in use in Jefferson County are running firmware version PC 1.96.4 with hardware that was previously certified by the state but has not yet been upgraded to meet VSS 2002 compliance, which is now required by the State. This earlier version of firmware is, of course, fully federally certified and has been used extensively in several other states; nevertheless it does not have a certification in the State of Kentucky. We have informed the Kentucky Secretary of State's office of this matter.

We deeply regret this error. After an internal review, we have determined that our procedures for verifying state certified versions prior to shipping and implementation were not followed in detail in this case. With your approval, and the State's, Premier will implement a plan to immediately correct this error by upgrading your AccuVote-OS units, hardware and firmware, to the current state certified versions (as identified above) at no cost to the county.

I believe you will find that through Jefferson County's logic and accuracy testing and post-election auditing that there have been no functional or performance issues resulting from the use of the earlier versions of firmware and hardware. However, please be assured that Premier's policy is to provide systems that fully meet all applicable state certification requirements. Again, we apologize for this oversight and look forward to working with you to schedule an upgrade of your AccuVote-OS equipment.

If you have any questions, please contact me at on my cell phone (214.280.6464.)

Sincerely:

A handwritten signature in black ink, appearing to read 'Ian S. Piper', written over a horizontal line.

Ian S. Piper
Compliance Officer
Premier Election Solutions, Inc.

CC: Trey Grayson (Kentucky Secretary of State)
 Dave Byrd (Premier President)
 Michael Lindroos (Premier Legal Counsel)
 Kathy Rogers (Premier Director of Gov't Affairs)
 Don Vopalensky (Premier State Certification Manager)

Johnson, Sarah Ball (SBE)

From: Shawn Merrick [SMerrick@JeffersonCountyClerk.org]
Sent: Thursday, August 23, 2007 10:52 AM
To: Johnson, Sarah Ball (SBE)
Cc: Susan Clark; Tom Barrow
Subject: Election Equipment Software Versions

Hello Sarah,

Here are the versions of election equipment software currently used in Jefferson County:

GEMS Server:	1.18.24.0
Accuvote-2000 (scanner):	1.96.4
Accuvote-TSX (touchscreen):	4.6.4
Voter Card Encoder:	1.3.2
VC Programmer (Card encoder for absentee TSX):	4.6.1

Please let me know if you have any other questions.

Shawn Merrick
Information Systems Manager
Jefferson County Board of Elections
502-574-6113



Louisville Metro Capital Improvement Program Fiscal Year 2005 - 2006

AGENCY: Board of Elections
PROJECT TITLE: Help America Vote Act (HAVA) Equipment
PROJECT NUMBER: 42
SCHEDULED START DATE: July 2005
SCHEDULED END DATE: June 2006

PROJECT DESCRIPTION:

Under the Help America Vote Act (HAVA) of 2002, we are required to have ADA compliant accessible voting equipment by January 2006. Subtitle A of HAVA states the voting system shall (A) be accessible for individual, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation as for other voters. (B) satisfy the requirement of subparagraph (A) through the use of at least one direct recording electronic voting system equipped for individuals with disabilities at each polling place. To comply with HAVA, 506 machines will be purchased at \$5,000 each.

PROJECT FUNDING	FY 2004 - 2005	FY 2005 2006	FY 2006 - 2007	FY 2007 - 2008	FY 2008 - 2009	FY 2009 - 2010	TOTAL
Capital Fund							-
Municipal Aid Program							-
County Road Aid Program							-
State		2,530,000					2,530,000
Federal CDBG							-
Other							-
TOTAL		2,530,000					2,530,000

PROJECT EXPENDITURE	FY 2004 - 2005	FY 2005 2006	FY 2006 - 2007	FY 2007 - 2008	FY 2008 - 2009	FY 2009 - 2010	TOTAL
Property Acquisition							-
Construction							-
Equipment		2,530,000					2,530,000
Personnel							-
Professional Services							-
Other							-
TOTAL		2,530,000					2,530,000



Louisville Metro Capital Improvement Program Fiscal Year 2005 - 2006

AGENCY: Board of Elections
PROJECT TITLE: AccuVote Scanners
PROJECT NUMBER: 41
SCHEDULED START DATE: July 2005
SCHEDULED END DATE: June 2006

PROJECT DESCRIPTION:

This capital project is for AccuVote scanners purchased in 1997. The scanners are housed at the Board of Elections Warehouse located at 1601 West Main Street. The voting system meets standards for electronic voting equipment. The precinct count optical scan system maintains accurate counts of votes cast by registered voters in an election.

PROJECT FUNDING	FY 2004 - 2005	FY 2005 - 2006	FY 2006 - 2007	FY 2007 - 2008	FY 2008 - 2009	FY 2009 - 2010	TOTAL
Capital Fund	233,500	233,500	233,500				700,500
Municipal Aid Program							-
County Road Aid Program							-
State							-
Federal CDBG							-
Other							-
TOTAL	233,500	233,500	233,500	-	-	-	700,500

PROJECT EXPENDITURE	FY 2004 - 2005	FY 2005 - 2006	FY 2006 - 2007	FY 2007 - 2008	FY 2008 - 2009	FY 2009 - 2010	TOTAL
Property Acquisition							-
Construction							-
Equipment	233,500	233,500	233,500				700,500
Personnel							-
Professional Services							-
Other							-
TOTAL	233,500	233,500	233,500	-	-	-	700,500

APPENDIX V

KENTUCKY REQUIREMENTS FOR VOTING SYSTEMS

The Role of the Attorney General

The Attorney General has the duty to enforce the state's election laws under KRS 15.243. The Office of the Attorney General ("OAG") maintains a toll-free Election Fraud Hotline throughout the year and during all hours that the polls are open for any election. KRS 15.243(2)(c). The Attorney General may initiate investigations upon request or on his own motion. KRS 15.243(2)(d). The Attorney General has the authority to mobilize the Auditor of Public Accounts, state and local law enforcement, and any other state and local agencies. Officials are required to give all possible assistance to the Attorney General in the performance of his duties. KRS 15.243(5).]

Kentucky's Constitution Guarantees the Secrecy of Every Vote

Kentucky Constitution § 147 guarantees that all elections "by the people shall be by secret official ballot, furnished by public authority to the voters at the polls, and marked by each voter in private at the polls, and then and there deposited."

The same provision also allows for "voting machines" that may be installed at the expense of the counties. *Id.*

Finally, it contains an express requirement for disabled voters: "The General Assembly shall pass all necessary laws to enforce this section and shall provide that persons illiterate, blind, or in any way disabled may have their ballots marked or voted *as herein required.*" *Id.* (emphasis supplied.)]

Kentucky Law Requires the State Board of Elections to Oversee the Certification and Installation of New Voting Systems

Kentucky election law places the authority to examine, certify and regulate electronic voting systems on the State Board of Elections. See: KRS 117.375 et seq.

KRS 117.377 requires counties to purchase only voting system equipment that has been approved by the State Board of Elections and requires the county to notify the State Board of Elections when "a new voting system" is installed.

KRS 117.379(1) provides that the State Board of Elections shall examine all voting systems before certifying them for use in any Kentucky county and empowers the State Board of Elections to reexamine any voting system already approved.

KRS 117.379(2) sets forth the examination or reexamination procedure, including the appointment of three (3) examiners:

- (1) An examiner who is an expert in computer science or electronic voting systems;
- (2) A person who is knowledgeable in election procedures and law in Kentucky; and
- (3) A person who is a present or former county clerk.

The examiners "shall submit one (1) written report on each system examined or reexamined to the State Board of Elections." Only a system that meets all of the requirements of KRS 117.381 shall be approved. KRS 117.379(2).]

KRS 117.381 provides the basic conditions for certification:

No electronic voting system shall, upon any examination or reexamination, be approved by the State Board of Elections unless it shall be established that such system, at the time of examination or reexamination:

- (1) Provides for voting in secrecy;
- (2) Permits each voter to vote at any election for all candidates and questions for which he is lawfully entitled to vote, and no others;
- (3) Permits each voter, at the general election to vote a straight political party ticket by one (1) or more marks or acts;
- (4) Provides a method for write-in voting;
- (5) Provides for a nonpartisan ballot;
- (6) If it is of a type that registers the vote electronically, the voting system shall preclude each voter from voting for more persons for any office than he is entitled to vote for or upon any question more than once;
- (7) Permits each voter at a primary election to vote only for the candidates seeking nomination by a political party in which such voter is registered, and for any candidate for nonpartisan nomination, and for any question upon which he is entitled to vote;
- (8) If it is of a type that registers the vote electronically, the voting system shall permit each voter to change his vote for any candidate or upon any question appearing on the official ballot up to the time that he takes the final step to register his vote and to have his vote computed. If it is of a type that uses paper ballots or ballot cards to register the vote and automatic tabulating equipment to compute such votes, the system shall provide that a voter who spoils his ballot may obtain another ballot;
- (9) Is suitably designed for the purpose used, is constructed of a durable material, and is safely transportable;
- (10) Is so constructed that a voter may readily learn the method of operating it; and
- (11) Meets or exceeds the standards for electronic voting equipment established by the Federal Election Commission; and
- (12) Provides for tabulating votes at the precinct in accordance with the requirements of KRS 117.275.

Finally, KRS 117.383 grants to the State Board of Regulations the exclusive regulatory authority regarding electronic voting devices and components and the procedures relating to these systems.

VOTING SYSTEMS RECORDS EXAMINED BY THE ATTORNEY
GENERAL

The Office of the Attorney General obtained records from the State Board of Elections detailing the most recent examination and certification of three (3) electronic voting systems:

- (1) The Hart InterCivic eSlate Voting System, software version 6.2.1 and its related components, certified by the State Board of Elections on December 19, 2006;
- (2) Diebold Election Systems, Inc.'s¹ AccuVote Optical Scan ("OS") (model D) with firmware version 1.96.6, Voter Card Encoder 1.3.2, AccuVote-OS Central Count firmware version 2.0.12, Key Card Tool 4.6.1 and VCProgrammer 4.6.1, which were all certified on August 16, 2005 and AccuVote-TSX DRE (Model D) Touch Screen (certified on September 19, 2006) with Ballot Station firmware version 4.6.4 (certified on March 21, 2006); and
- (3) The ES&S Unity 3.0.1.1 and related components.

¹ Now Premier Election Solutions, Inc.



COMMONWEALTH OF KENTUCKY
OFFICE OF THE ATTORNEY GENERAL

GREGORY D. STUMBO
ATTORNEY GENERAL

CAPITOL BUILDING, SUITE 118
700 CAPITOL AVENUE
FRANKFORT, KY 40601-3449
(502) 696-5300
FAX: (502) 564-2894

October 2, 2007

Via facsimile & hand-delivery

Secretary of State Trey Grayson
Chairman, State Board of Elections
Suite 152, State Capitol
700 Capitol Avenue
Frankfort, Kentucky 40601

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

Dear Secretary Grayson:

As I promised at the State Board of Elections meeting on September 18, 2007, I am submitting to you and the Board the enclosed expert report – *Improving Kentucky's Electronic Voting System Certifications*. This report confirms my investigative findings that the Board's certification process is insufficient to test the security and accuracy of Kentucky's electronic voting systems. While I am pleased that my inquiries led the Board (1) to reexamine Kentucky's voting systems and (2) to provide more comprehensive "best practices" training to county clerks and poll workers, this report clearly shows that there is more we can do to ensure the integrity of Kentucky elections.

The report recommends that the Board take immediate action to:

- Develop written policies & procedures for the protection of voting machines in all counties in the Commonwealth, consistent with the recommendations of the California Secretary of State; and
- Demand that voting machine manufacturers implement all the fixes to Kentucky's voting systems that they will have to provide in other states as a result of top-to-bottom reviews of these systems.

Despite recommendations by my office, the SBE did not require these protections during the recertification process.

Regarding future actions, the report recommends the following:



October 2, 2007

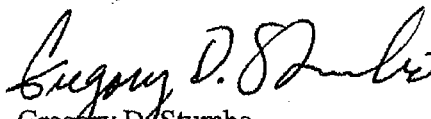
Page2

- The SBE's certification process for electronic voting systems must be dramatically improved;
- Vendors should be required to provide the source code and specific design documents for their proprietary software, subject to reasonable non-disclosure agreements, so that the SBE or its designated expert examiners may conduct a thorough study of the systems;
- Optical scan systems ("OS") that use paper ballots with accessible marking devices for the disabled should be encouraged, since proposed Federal legislation will require these types of systems (The Secretary of State's recent statements that he is willing to commit \$15 million in HAVA funds towards this goal is encouraging, but simply not enough. Additional federal funds must be secured.);
- The SBE should implement mandatory random post-election audits and recount procedures that compare the machine-generated vote totals with the actual voters' paper ballots consistent with the recommendations by the Brennan Center/Samuels Law report, *Post-Election Audits: Restoring Trust in Elections* (2007); and
- The SBE should work with counties to develop in-house expertise in the area of ballot programming and electronic voting systems in order to reduce the risks of 100% reliance on vendor support.

It is my hope that the SBE will implement this expert advice and present any legislative initiatives required to the 2008 General Assembly.

My office will carefully monitor the upcoming 2007 General Election and will have expert legal and technical advice available in case of any compromise of our voting systems. My one and only aim is to increase public confidence in our elections. I look forward to continuing to advise you and the Board about achieving this for Kentucky.

Sincerely,



Gregory D. Stumbo
Attorney General

Enclosures:

Epstein, *Improving Kentucky's Electronic Voting Systems Certifications*

C: Sarah Ball Johnson

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 Diebold¹ 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 study², 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 2002³). 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 tests⁴. As noted by Professor Michael Shamos⁵, 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 reports⁶ 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 recommendations⁷, 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 Florida⁸ 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 votes⁹, 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 calibration¹⁰, 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 name¹¹.
 - 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 report¹², 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 quality¹³. 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 fade¹⁴. Kentucky law only requires keeping paper for 60 days¹⁵, 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 paper¹⁶.
- 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 test¹⁷.
- 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 infrared¹⁸, 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 notes¹⁹ “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” problems²⁰ 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 election²¹. 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 conditions²².
- 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/tibr/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/tibr/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 site²³. 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 scenario²⁴, 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 machines²⁵. 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 studies²⁶.

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 audits²⁷ 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 School²⁸.
- 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

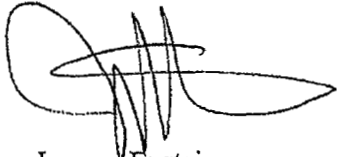
²⁷ The term "random audit" in this context means a selection of random precincts at every election, and a manual comparison of the vote totals generated by the voting equipment with physical paper ballots (be they optical scan or VVPAT). This should occur regardless of whether there are any observed 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,

A handwritten signature in black ink, appearing to read 'Jeremy Epstein', with a large, stylized initial 'J'.

Jeremy Epstein
4575 Forest Drive
Fairfax VA 22030

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

BIOGRAPHY OF JEREMY EPSTEIN
Electronic Voting Systems Expert &
Consultant to the Office of the Attorney General

Jeremy Epstein leads the product security department at Software AG, a leading provider of business integration software, where he is responsible for meeting security requirements for many of the world's largest corporations and government agencies. Mr. Epstein has twenty years experience in information security research, product development, and consulting, including serving as consultant to Cyber Defense Agency, LLC, a leader in the area of cyber security.

In the area of electronic voting, Mr. Epstein is an independent consultant who has served on two Virginia legislative panels investigating what the Commonwealth should be doing, co-founded Virginia Verified Voting (a lobbying group for safer electronic voting), been an expert reviewer for the nationally recognized Brennan Center report on voting system security, *The Machinery of Democracy: Protecting Elections in an Electronic World* (Brennan Center, June 2006), and is currently the expert witness for voting technology in a case against the State of Maryland. He's given speeches on electronic voting at a half dozen universities, and participates in several voting working groups. He recently published an article in *IEEE Computer* on how electronic voting machines work.

Mr. Epstein led teams that developed one of the first multi-level secure UNIX operating systems, the first high assurance multi-level secure windowing system, and the first Orange Book evaluation of a network operating system (Novell NetWare). He has been involved in standards committees that have developed SAML, XKMS, and POSIX Security.

Mr. Epstein has published over 20 articles in peer-referenced conferences and journals, and was program chair of the Annual Computer Security Applications Conference for 3 years. He's served on National Science Foundation (NSF) proposal review panels and advised the Defense Advanced Research Projects Agency (DARPA) on research directions.

Jeremy holds a B.S. in Computer Science from New Mexico Tech, an M.S. in Computer Sciences from Purdue University, and completed coursework for a PhD in Information Security at George Mason University.