COMMONWEALTH OF PENNSYLVANIA

DEPARTMENT OF STATE

EXAMINATION RESULTS OF THE DIEBOLD ELECTION SYSTEMS' ACCUVOTE TSX ELECTRONIC VOTING SYSTEM, OS OPTICAL SCAN UNITS AND GEMS ELECTION MANAGEMENT SOFTWARE

Issued by:

Pedro A. Cortés

Pedro A. Cortés
Secretary of the Commonwealth
December 22, 2005

EXAMINATION OF THE DIEBOLD ELECTION SYSTEMS' ACCUVOTE TSX ELECTRONIC VOTING SYSTEM, OS OPTICAL SCAN UNITS AND GEMS ELECTION MANAGEMENT SOFTWARE

A REPORT BY THE SECRETARY OF THE COMMONWEALTH OF PENNSYLVANIA

I. INTRODUCTION

Article XI-A of the Pennsylvania Election Code, 25 P.S. § 3031.1 et seq., authorizes the use of electronic voting systems. Section 1105-A of the Election Code, 25 P.S. § 3031.5, requires all electronic voting systems to be examined and approved by the Secretary of the Commonwealth before use in any election in Pennsylvania.

Upon the request for an examination of the AccuVote TSX Direct Recording Electronic Voting System, OS Optical scan units, and Guardian Election Management System (GEMS) election management software (hereinafter referred collectively to as the "System") made by Diebold Election Systems, Inc. (Diebold), the Department of State (Department) scheduled an examination of the System for November 22, 2005. The Department has received confirmation from Ciber, Inc. and Wyle Laboratories, Inc., federally recognized independent testing authorities (ITAs), that the System's hardware and software have successfully completed qualification testing in compliance with the Federal Election Commission 2002 Voting System Standards.

The Secretary of the Commonwealth retained Michael Ian Shamos, Ph.D., J.D., as a consultant to conduct an electronic voting system examination on November 22, 2005. Harry A. VanSickle, Commissioner of the Bureau of Commissions, Elections and Legislation; Kenneth A. Rapp, Deputy Secretary for Regulatory Programs; Larry Boyle, Deputy Chief Counsel; Chet Harhut, HAVA Administrator; Lindsley Houser, HAVA Assistant; Jim Criss, Bureau of Management Information Systems; Jonathan Marks, Chief of the Division of Elections/Precinct Data; and Barbara Levin, Legal Assistant; represented the Secretary of the Commonwealth.

II. SYSTEM PRESENTED FOR CERTIFICATION

Presented for certification were the following:

- AccuVote OS Model D optical scan precinct reader 1.96.6
- AccuVote OS optical scan central count reader CC 2.0.12
- AccuVote TSX touch-screen voting machine 4.6.4 without VVPAT
- GEMS election management system software 1.18.25

- GEMS election management system central server hardware
- Voter card encoder 1.3.2
- ST-100 access card writer
- VC Programmer 4.6.1
- Key Card Tool Software
- Election Media Processor 4.6.1
- Electronic Poll Book 4000 with firmware 1.1.5.0

The following paragraphs in this section briefly describe the functions of the System as summarized by the consultant.

Diebold presented two types of voting machines: a touch-screen DRE, the AccuVote TSX (TSX), and two optical scan devices, the AccuVote OS precinct reader and the AccuVote OS central count reader.

The TSX employs touch-screen hardware and is accessible to visually impaired voters through an audio interface and Americans with Disabilities Act (ADA) scroll buttons, and is also accessible to wheelchair-bound voters.

Upon opening the polls, the TSX must be initialized for voting by the insertion of a "smart" card known as a voter access card. This card contains information about the particular ballot style to be presented to the voter.

The vendor presented two models of AccuVote OS for examination, one for precinct count and one for central count. The Model D optical scan unit is able to handle multiple ballot styles and sizes, and reads both the front and the back of a ballot in a single pass.

GEMS is a comprehensive program that allows a jurisdiction to set up and manage all of its Diebold voting machines, including loading them with election-specific data and accumulating results. It provides the following functions, among others:

- Builds a geographic database for political subdivisions such as precincts.
- Builds election-specific databases containing party names, office titles, candidate names and question text.
- Lays out optical scan and DRE ballots.
- Maintains an inventory of voting machines and assigns them to specific precincts.
- Accumulates results.
- Produces printed reports.

The voter card encoder, ST-100, VC Programmer and Key Card Tool are components for producing smart cards that are needed to access various voting machine functions and to activate the touch-screens for voting.

The Election Media Processor is a separate computer that is able to read multiple Personal Computer Memory Card International Association (PCMCIA) cards simultaneously and upload

their contents to GEMS. It is intended to speed the process of accumulating results on election night.

The Electronic Poll Book (EPB) would ordinarily be considered a voter registration system and not subject to certification under the electronic voting provisions of the Pennsylvania Election Code. The EPB can be used to generate voter access cards, which are smart cards used to activate voting machines with a ballot style specific to the voter. Because EPB writes cards that interact directly with a voting system, it becomes part of the voting system and is therefore subject to certification.

The vendor recommends that GEMS be a standalone system dedicated only to election functions. However, even in this recommended configuration it is connected to an unconstrained local area network. The vendor also recommends that GEMS not be connected either to the Internet or to a jurisdiction's intranet.

In a touch screen jurisdiction, one TSX must be present at the county for use with GEMS. The TSX is used to proofread and test the ballot. A variety of devices are connected electrically to the central server at various times. TSX is connected via a network interface. An optical reader can be directly cabled to the GEMS server for reading absentee ballots, which is not permitted in Pennsylvania. The scanner can also validly be used to test opscan ballots and to verify timing marks. The ST-100 card burner also cables directly to GEMS.

III. EXAMINATION PROCEDURES AND RESULTS

At the examination conducted on November 22, 2005, the consultant tested the System for the statutory requirements specified in section 1107-A of the Election Code, 25 P.S. § 3031.7. The vendor demonstrated the setup, opening of the polls, voting, closing of the polls and election night tabulation features of the System. The consultant and the Department representatives asked questions of the vendor and requested demonstrations of various features before conducting the Pennsylvania Standardized Test (Test). The first Test is a set of 12 Municipal Election ballots. The second Test is a set of 12 Municipal Primary ballots (6 Democratic and 6 Republican). Both Tests are designed to ensure the electronic voting System's compliance with the Election Code.

Although the System accurately tabulated the results of the Test, based on the results of the examination, including the answers to questions provided by the vendor and the advice provided by the Department's consultant, the Department offers the following observations, concerns and conditions for the System.

The VVPAT

To comply with statutory requirements in other states, Diebold has added a "Voter-Verified Paper Audit Trail" (VVPAT) printer called AccuView as an optional component for the TSX unit. The consultant explained to the vendor that continuous roll VVPATs cannot be certified in Pennsylvania. The "numbered list of voters" is a list of voters listed in the order in which they voted. This document is considered public information and is available for inspection by the public at each county board of elections upon request. Furthermore, nothing prevents a volunteer authorized by a candidate or political party as a "watcher" from remaining all day in the polling place and recording the order of voters, and, if necessary, on which machine they voted. Because the ballot images are recorded on paper in the order in which they are voted, merely comparing each ballot image with the numbered list of voters will reveal every voter's choices in a given precinct. Such a comparison could easily be made in the event of a recount. This is a direct violation of Article VII, Section 4 of the Pennsylvania Constitution, which mandates that "[a]ll elections by the citizens shall be by ballot or by such other method as may be prescribed by law; Provided, That secrecy in voting be preserved." This also violates section 1107-A(1) of the Election Code, 25 P.S. § 3031.7(1), which states that no electronic voting system can be approved unless it "provides for voting in absolute secrecy and prevents any person from seeing or knowing for whom any voter, except one who has received or is receiving assistance as prescribed by law, has voted or is voting."

The vendor was aware that certification of the VVPAT was unlikely. Therefore, Diebold did not offer the AccuView for certification on November 22, 2005. **Regardless, the Secretary reiterates that the AccuView continuous roll VVPAT must be disabled or removed prior to being delivered to Pennsylvania counties because it violates the Pennsylvania Constitution and the Election Code.**

Security of the System

Some aspects of the System design have negative security implications. Failure to incorporate strong security controls violates section 1107-A(12) of the Election Code, 25 P.S. § 3031.7(12), relating to ballot security procedures.

It is common for vendors to add various communication interfaces to their devices for a variety of purposes, including uploading of vote totals and downloading of software patches. While the Pennsylvania Election Code does not deal specifically with modems and other particular communication methods, the general requirement of security in section 1107-A(12) of the Election Code, 25 P.S. § 3031.7(12), requires the Department to consider these devices. The Department has always taken the position, based on the statute, that modem communication from a voting system of results, either official or unofficial, is impermissible. Doing so requires connection of uncertified equipment (the telephone instruments and network) to certified equipment (the voting machines and tabulators). The resulting configuration is not certified, and therefore, cannot be used in elections.

Furthermore, the use of voting systems that run on general-purpose laptops having wireless interfaces, Internet connections, local area network (LAN) interfaces and modems can be problematic. None of these are authorized for use in voting systems in Pennsylvania, except completely standalone LANs, in which the only components connected are certified items of voting equipment. Even connecting a voting system computer to a county's administrative LAN is forbidden, because such a connection provides an unsupervised and unauditable channel of attack on the voting. **For this reason, Pennsylvania counties purchasing the Diebold System may not use modems provided by Diebold in the precinct to transmit official or unofficial election results.**

The vendor explained that their ballot precinct counters use a universal key with a locking mechanism, and only four different versions have ever been created. This means that a person might easily obtain a key to unlock the machine. There are conveniences to having universal keys, but unfortunately they also make tampering more convenient. **Therefore, the Secretary recommends that Diebold consider changing the locking system on its scanners so that there are many different locks and different keys.**

AccuVote OS precinct and central count optical scanners

The consultant tested the precinct count unit first. The Department provided the vendor with a sample election, which was programmed into the unit. Initially, the scanner was placed in test mode and a blank ballot was read. The unit then produced a report indicating that no marks were present on the ballot. Next, a fully voted ballot was read, and the unit produced a report listing all the voting positions that were marked. Ballots for the test general election and the test primary election were run through the machine and tabulation reports were produced. The tabulation results were correct.

Then, the consultant tested the OS unit with central count firmware. In this mode, the counter is networked to a GEMS server and ballot images are sent to the server for interpretation and tabulation. The test was performed using the same ballots that had been read correctly by the precinct unit.

The first general election ballot scanned was problematic. The ballot was rejected as over-voted, despite the fact that it contained only a single mark in the straight-party office. Several other ballots were also rejected resulting in incorrect totals. The vendor was not able to offer any explanation for this malfunction. The vendor tried the experiment a second time, and this time, the machine read all the ballots correctly and produced a correct tabulation. The vendor performed the experiment a third time, and the totals were again correct.

Next, the primary election ballots were counted. No ballots were rejected, but the totals produced were incorrect. All of the vote totals for Republicans candidates were correct, but almost all the Democratic totals were wrong. (The only correct one was for a total of zero, which was only fortuitously correct.) On a second attempt, the totals were wrong again, but were different from the ones obtained the first time.

The vendor hypothesized that the scanner unit was faulty. Since the only difference between a precinct count machine and a central count machine is the installed firmware, the vendor moved the central count firmware to the machine that had performed properly as a precinct count device. When this change was completed, the primary ballots were read correctly.

While it was possible to obtain correct results, the source of the problem remains unexplained. If the error had manifested itself after pre-election testing, it would not have been detected. There was no outward sign, such as an error message, that ballots were not being tabulated properly. If the problem lay in the scanning portion of the machine, it is not clear what would account for results being different on subsequent readings.

Both scanners did tabulate the ballots correctly. However, the following has come to the Secretary's attention.

In June 2005, Finnish security expert Harri Hursti demonstrated that the memory card used in the AccuVote OS units can contain executable code, and that furthermore, the scanners will execute the code if it is present. Hursti was able to use this fact to program a memory card so that it (1) contained counters that were not zero and, in fact, had counters with negative vote totals; (2) produced a zero tape nevertheless; and (3) used the negative counter values to subtract votes from candidates and positive counter values to add votes to candidates, which resulted in a complete manipulation of the election. Note that if the sum of the negative and positive counter values are zero, the total number of votes tallied will exactly match the total number cast, and nothing will appear to be amiss. Hursti was able to disguise the behavior so it would not be detected in pre-election or post-election testing. (A manual recount would reveal this.)

One of the conditions that allowed the Hursti programming to be performed is the ability to program a zero report that does not even look at the counters that are supposed to be zero. A fix would be to hard-code a zero report into the OS firmware so that there is assurance that the counters are actually being examined and displayed. **In light of the findings by Harri Hursti and the performance anomalies of the scanners noted above, the Secretary denies certification for the AccuVote OS precinct and central count scanners.**

Electronic Poll Book 4000

The EPB is a computer that runs Windows CE. The EPB has a power cord and multiple interface ports, including Universal Serial Board (USB), serial, Firewire, LAN, PCMCIA, headphones and flashcard. It can also accommodate a barcode scanner to scan identity credentials such as drivers' licenses.

Proper use, in compliance with HAVA, clearly requires an interface to the statewide voter registration system, the Statewide Uniform Registry of Electors (SURE) in the case of Pennsylvania. This means that a customized interface must be developed that would allow the download of registration data to the counties in compliance with state law. Before any registration system that interacts with a voting system can be certified, such capability would have to be demonstrated. **Therefore, the Secretary is deferring a decision on certification of**

the Electronic Poll Book 4000 until it can be demonstrated that it can be successfully integrated with the SURE system.

GEMS

A peculiar aspect of GEMS is that while it offers a large variety of reports, none of them produce a tabulation that lists every candidate that was voted for, including write-in candidates, along with their vote totals. This information can now only be assembled by manual collation of different reports. For example, the "Summary Report" does not show write-in names. The report "Write-In Summary By Race" shows all write-in votes, but does not indicate whether multiple votes for the same candidate appeared on the same ballot (in a vote-for-many office). The report "Write-In Detail By Ballot" shows which ballot the write-ins appeared on and can thus be used to eliminate multiple votes on the same ballot, but it does not show vote totals. The report "Write-In Detail by Race" is useful, but does not show anything other than write-in candidates. In order to report an election properly, it is necessary to print a Summary Report and a Write-In Detail by Race report and merge them by hand.

The summary reports are not completely accurate because they truncate data. Sometimes a candidate's party affiliation is shown, sometimes not. For example, in one of our test elections, candidates Smith and Allen were shown as Republicans but candidate Johnson, also a Republican, had no party affiliation listed on the Summary Report. This appeared to be related to the length of the candidate's name, but no warning was given on the report that anything had been omitted. Cross-filed candidates, which are common in Pennsylvania, were listed as not having any party affiliation, which is incorrect. **The Secretary recommends that when GEMS produces reports from the internal ballot images by different system components, the reports must display candidate names, party affiliations and all other essential ballot information identically.**

Similarly, there were differences between the ballot images printed from the TSX units and those uploaded to GEMS from the same machines. These differences also appeared to be caused by inappropriate truncation of names and party affiliations. If an audit trail is to function properly, it must be absolutely reliable. The fact that the same audit trail looks different when printed on two different machines reduces confidence in the audit trail to a negligible level. **The Secretary recommends that GEMS produce a combined summary report showing names of write-in candidates receiving votes along with vote totals for all other candidates.**

IV. RECOMMENDATIONS/CONDITIONS FOR CERTIFICATION

Recommendations for Certification

The Secretary of the Commonwealth is awarding certification for the following components of the System:

- AccuVote TSX touch-screen voting machine 4.6.4 without the AccuView VVPAT

- GEMS election management system software 1.18.25.
- GEMS election management system central server hardware
- Voter card encoder 1.3.2
- ST-100 access card writer
- VC Programmer 4.6.1
- Key Card Tool Software
- Election Media Processor 4.6.1

The preceding components of the Diebold System are granted certification under the following conditions:

1. No components of this System shall be connected to any modem or network interface, including the Internet, at any time, except when a standalone local area network configuration in which all connected devices are certified voting system components is used. Transmission of unofficial results can be accomplished by writing results to media, and moving the media to a different computer that may be connected to a network.

2. The Diebold System was not shown with a VVPAT. Therefore, all TSX machines sold in the Commonwealth must either have the VVPAT disabled or removed.

The Secretary is also recommending that subsequent versions of the Diebold System, submitted for certification in Pennsylvania, meet the following conditions:

1. All reports produced from the internal ballot images by different system components should display candidate names, party affiliations and all other essential ballot information identically.

2. Locks on voting machines and scanners, particularly the Model D, should be keyed differently. At present, a very small number of master keys can open any Diebold unit in the country, which is a security risk.

3. GEMS should produce a combined summary report showing names of write-in candidates receiving votes, along with vote totals for all other candidates.

Deferral of Certification

The Secretary of the Commonwealth is deferring certification of the Electronic Poll Book 4000 until it can be demonstrated that it can be successfully integrated with the SURE system.

Denial of Certification

Pursuant to the concerns mentioned in Section III of this report certification is being denied for the following components:

- AccuVote OS Model D optical scan precinct reader 1.96.6
- AccuVote OS optical scan central count reader CC 2.0.12

V. CONCLUSIONS

As a result of the examination conducted on November 22, 2005, and after consultation with the Department's staff and consultant, certification of the TSX electronic voting system with GEMS election management software is hereby awarded by the Secretary of the Commonwealth for use in elections in the Commonwealth of Pennsylvania, in accordance with section 1105-A of the Election Code, 25 P.S. § 3031.5, **provided it is implemented with the conditions listed in Section IV of this report.** The System will accommodate no more than 350 voters per unit. **In addition, the Secretary of the Commonwealth is denying certification of the AccuVote OS precinct and central optical scan readers for the reasons listed in Section III.**

In addition, pursuant to the Directive on Electronic Voting Systems issued by the Secretary of the Commonwealth on July 22, 2005 and to section 1105-A(d) of the Pennsylvania Election Code, 25 P.S. § 3031.5(d), this certification is valid only for the voting system examined on November 22, 2005. If the vendor makes *any* changes to the system subsequent to November 22, 2005, it must *immediately* notify both the Pennsylvania Department of State and the relevant federal ITAs or their successors. Failure to do so may result in the decertification of this voting System in the Commonwealth of Pennsylvania.

All jurisdictions implementing this System for use must comply with the requirements and conditions found in this report and any directives issued by the Secretary of the Commonwealth regarding the use of this System, in accordance section 1105-A(a-b) of the Pennsylvania Election Code, 25 P.S. § 3031.5(a-b).