

COMMONWEALTH OF PENNSYLVANIA

DEPARTMENT OF STATE

AMENDED

**CERTIFICATION OF THE DIEBOLD ELECTION SYSTEMS'
ACCUVOTE TSX DIRECT RECORDING ELECTRONIC VOTING
SYSTEM AND CERTIFICATION OF THE ACCUVOTE OS OPTICAL
SCAN CENTRAL COUNT READER CC 2.0.12**



Issued by:

Pedro A. Cortés

Pedro A. Cortés
Secretary of the Commonwealth
January 17, 2006

AMENDED
CERTIFICATION OF THE DIEBOLD ELECTION SYSTEMS'
ACCUVOTE TSX DIRECT RECORDING ELECTRONIC VOTING
SYSTEM AND CERTIFICATION OF THE ACCUVOTE OS OPTICAL
SCAN CENTRAL COUNT READER CC 2.0.12

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 (TSX), OS Optical scan units (OS), and Guardian Election Management System (GEMS) election management software produced by Diebold Election Systems, Inc. (Diebold), the Department of State (Department) scheduled an examination of the System for November 22, 2005. The Department had received confirmation from Ciber, Inc. and Wyle Laboratories, Inc., federally recognized independent testing authorities (ITAs), that the System's hardware and software had 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.

On December 22, 2005, the Secretary of the Commonwealth certified the TSX electronic voting system with GEMS software for use in elections in the Commonwealth of Pennsylvania, in accordance with section 1105-A of the Election Code, 25 P.S. § 3031.5 and issued a report. As stated in the conclusion of that certification report, the Secretary based his decision on the results of the examination conducted on November 22, 2005, as well as consultation with the Department's staff and consultant.

Since the certification on December 22, 2005, new facts have come to light regarding TSX, as detailed in Section II of this Report. Based on these facts, the Secretary of the Commonwealth amends the original certification of both TSX and GEMS (hereinafter referred to as the "System"), as detailed in the Conclusion in Section III of this Report.

For the reasons stated below, the Secretary also grants certification to the AccuVote OS optical scan central count reader CC 2.0.12.

II. NECESSITY TO REVIEW AND AMEND THE DIEBOLD CERTIFICATION

When the Secretary of the Commonwealth certified both TSX and GEMS on December 22, he denied in the same report certification of the AccuVote OS Model D optical scan precinct reader 1.96.6 and AccuVote OS optical scan central count reader CC 2.0.12, primarily because of a security vulnerability known as the "Hursti exploit." The following is a description of the "Hursti exploit" and its implications for the AccuVote OS optical scanners, taken from page 7 of the Secretary's report of December 22, 2005:

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.** (Emphasis in original.)

The Hursti exploit comprises two steps: (1) preparation of an OS memory card in which the candidate counters do not begin at zero; and (2) substitution of fake zero totals report code which, when executed by the OS unit, falsely reports that the totals are zero when they are not.

Using the Hursti exploit, the official vote totals, which are the totals tapes produced by the precinct OS and signed by the election judges, can be manipulated at will.

Shortly after the Secretary's report was issued on December 22, Dr. Shamos became aware that the Hursti vulnerability may also be present in TSX, based upon a report of Steven V. Freeman, a consultant to the California Secretary of State. This report (the "Freeman Report") notes on p. 7 that the same AccuBasic reporting mechanism (which allows the Hursti exploit) is present in both OS and TSX.

Upon reviewing the Freeman Report, Dr. Shamos examined the TSX source code provided to him by Diebold, and verified that TSX contains an AccuBasic interpreter and operates on .abo files in a manner similar to that of OS. When Dr. Shamos notified the Department of his findings, the Secretary immediately requested a reexamination of the Diebold System. The Department, as part of the reexamination, also contacted Diebold officials and scheduled a conference call for Tuesday, January 3, 2005, to determine whether the Diebold System remained in compliance with the relevant state and federal requirements for electronic voting systems.

As a result of that conference call on January 3, with Diebold and Department officials, including the Department's consultant, Diebold answered the Department's questions in a letter dated January 5, 2006. These questions and answers are attached to this report as Appendix A and are discussed further in the sections below, regarding both the state and federal requirements and standards for electronic voting systems.

Federal Voting System Test Requirements and Standards

Section 1105-A(a) of the Pennsylvania Election Code, 25 P.S. § 3031.5(a), contains two requirements for electronic voting systems:

- 1) They must be approved by a federally recognized independent testing authority (ITA);
and
- 2) They must meet federal test standards.

As noted above, the Department had received confirmation from Ciber, Inc. and Wyle Laboratories, Inc., federally recognized independent testing authorities (ITAs), that both TSX and GEMS had successfully completed qualification testing. The next step is to examine the federal voting system test standards themselves.

The current federal voting system test standards are the Federal Election Commission 2002 Voting System Standards, available at http://www.eac.gov/election_resources/vss.html. Performance standard 4.2.2, "Software Integrity," reads: "Self-modifying, dynamically loaded, or **interpreted code is prohibited**, except under the security provisions outlined in section 6.4.e. This prohibition is to ensure that the software tested and approved during the qualification process remains unchanged and retains its integrity." (Emphasis added.) There is no section 6.4.e, which appears to have been a typographical error, apparently meant to refer to 6.4.1(e).

Section 6.4.1 is entitled: "Software and Firmware Installation." It provides:

"The system shall meet the following requirements for installation of software, including hardware with embedded firmware:

- a. If software is resident in the system as firmware, the vendor shall require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations;
- b. To prevent alteration of executable code, no software shall be permanently installed or resident in the system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware;
- c. The system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote-counting program, and its associated exception handlers;
- d. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as computer chip) other than the component on which the operating system resides; and
- e. After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible."

AccuBasic is a power report-writing language used by Diebold to enable it to customize reports produced on its voting systems without the need to change overall system source code, which in turn would necessitate additional testing by an ITA. AccuBasic source code is compiled using a compiler run at Diebold that is not available to any election jurisdiction. In particular, this compiler is not part of GEMS. The compiler produces AccuBasic "object code" in the form of .abo files, although it is not object in the usual sense because it does not consist of native machine instructions. It is more closely analogous to Java bytecode, which itself is neither source nor object code, but is code that can only be executed by an interpreter. Likewise, AccuBasic .abo files are designed to be executed by an interpreter resident in the TSX unit.

The .abo files are loaded by GEMS onto memory cards, which are supposed to be inserted into TSX and sealed in place in the warehouse. When a report is requested at the precinct, the relevant .abo file is interpreted by the onboard interpreter and executed to produce the report. In this way, Diebold can alter the content and appearance of reports without changing the code of GEMS or TSX.

AccuBasic is an interpreted code language because it is neither source nor object code and cannot run on TSX without the presence of an interpreter. The Diebold source code contains a module named abinterp.cpp, whose introduction states that it "implements the Accu-Vote Basic (A-Basic) interpreter." A later comment in the same code claims that "A-Basic is a relatively rich language, supporting the normal flow control statements, string and integer data types, strings and integer expressions, and read-only access to all the data contained on the memory card." Thus, AccuBasic allows introduction of interpreted code into a voting system, which contravenes Performance Standard 4.2.2, unless it is compliant with 6.4.1.

Regarding 6.4.1(a), the AccuBasic interpreter is resident as firmware on the TSX, but the code to be interpreted is on the memory card, not in firmware. Thus 6.4.1(a) is not applicable.

Likewise, 6.4.1(b) is not applicable because the AccuBasic programs, as opposed to the interpreter, are not “permanently installed or resident in the system.” 6.4.1(c) and (d) by their own terms are not applicable to AccuBasic.

6.4.1(e) is applicable. It states that after Election Day testing, no source code shall be resident or accessible. The “source code” in this case is the input to the interpreter, namely the .abo file. The code becomes “accessible” if some person has the ability to replace the TSX memory card after it has been installed in the TSX and subjected to pre-election testing.

However, that is precisely what the Hursti exploit involves, which is altering the interpreted code after Election Day testing has been performed. In OS (precinct readers) utilizing memory cards, this is problematic since it provides a mechanism for altering vote totals. During the conference call with Diebold representatives held on January 3, 2006, Diebold was asked to explain why the Hursti exploit is not possible or feasible on TSX. Diebold responded to these questions in its letter of January 5, 2006 (attached as Appendix A).

The OS and TSX differ in an important respect. The OS memory card contains counters corresponding to ballot positions. One prong of the Hursti exploit involves pre-loading these counters with negative numbers and producing a zero report that does not look at the counters but instead slavishly reports that all of them are zero.

A TSX memory card does not contain counters. Instead, it is a repository for full ballot images. When a tabulation is needed, the ballot images are tabulated on the spot, and no counters are maintained on the card. Producing a “zero report” on TSX effectively means adding up the votes for each candidate from the ballot images, without reference to any counters that may be stored on the card. Since there are no ballots on the memory card prior to the election, these totals would be zero.

The TSX also differs from OS in that the contents of the memory card are digitally signed by GEMS when the card is generated. After that point, no one can usefully alter the card contents. If one were to do so, the card would not be accepted at boot-up by TSX since it would not bear the correct digital signature.

The only feasible way to create an altered card that would be accepted by TSX would be to produce it on GEMS, which is able to produce correct digital signatures. But there is no apparent way to generate cards that have ballot images pre-loaded. Even if one were able to load the card with an .abo file corresponding to a fake totals report, the totals produced by TSX as a result of the manipulation would not correspond to totals produced back at the county when the memory card is uploaded. Therefore, any attempt to perform the Hursti exploit on TSX will fail even if .abo files can be altered.

Pennsylvania Voting System Requirements and Standards

Having examined the federal voting system test requirements and standards, it is appropriate to turn to the Pennsylvania Election Code to determine the standards and requirements for electronic voting systems in the Commonwealth of Pennsylvania.

Section 1107-A(16)(iii) of the Election Code, 25 P.S. §3031.7(16)(iii), requires that the system “shall be equipped with an element which generates a printed record at the beginning of its operation which verifies that the tabulating elements for each candidate position and each question and the public counter are all set to zero and with an element which generates a printed record at the finish of its operation of the total number of voters whose ballots have been tabulated, the total number of votes cast for each candidate whose name appears on the ballot, and the total number of votes cast for, or against, any question appearing on the ballot.”

TSX does not have “tabulating elements” as contemplated by the statute. The closest analogy would be to verify that there are no ballot images on the memory card prior to the beginning of operation. Even if the memory card contains rogue .abo files, it is still possible to verify that there are no ballot images present on the card by inspecting the public counter. The value of the public counter is determined by TSX firmware that does not rely or depend on any .abo files on the memory card. The contents of the card and the machine memory are compared and if any ballots are present the public counter will not read zero. In addition, if there is any discrepancy between the card contents and the TSX memory, the machine will not permit further voting. These functions are independent of any AccuBasic files. Therefore, if any ballots have been pre-loaded by whatever means, they will be detected at this stage, and it will not be necessary to rely on the standard zero report.

As discussed, even if the .abo file corresponding to the zero report is altered, it will still not be possible to affect the outcome of voting because of differences between OS and TSX. Therefore, TSX does not violate section 1107-A(12) of the Election Code, 25 P.S. §3031.7(12), relating to tampering of ballots.

AccuVote OS Central Count System

Based upon the consultant’s original report of December 14, 2005 in which he recommended that the AccuVote OS Central Count system (central count system) not be certified because of concerns over the Hursti exploit, the Secretary did not certify this central count system in his original certification of December 22, 2005. Since that certification, however, Diebold has pointed out, and the consultant has verified, that no AccuBasic interpreter exists in the central count system. Hence the Hursti exploit is not possible in that system. The scanner is connected directly to GEMS and its reports are produced directly on GEMS and not through any use of AccuBasic. Because the central count system otherwise passed tests conducted during the examination held on November 22, 2005, it is now certified.

III. CONCLUSIONS

Sections 1105-A(a) & (b) of the Election Code, 25 P.S. § 3031.5(a) & (b), provide that the Secretary of the Commonwealth, on his own initiative, may reexamine any electronic voting system that he previously examined and approved. The Secretary of the Commonwealth determined that sufficient concerns existed to reexamine the Diebold TSX and GEMS components.

This reexamination consisted of the following measures:

1. The Secretary requested that this matter be examined with Diebold officials, Dr. Shamos and representatives of the Department of State in a conference call held on Tuesday, January 3, 2006.
2. Diebold, by letter dated January 5, 2006, responded, to the satisfaction of the Secretary and his consultant, to the questions raised by the Department and its consultant on January 3, 2006. (A copy of this letter is attached as Appendix A.)
3. The Secretary requested that Dr. Shamos reexamine the Diebold system source code, review the answers provided by Diebold and issue a report to the Department, which he completed on January 7, 2006.

Award of 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
- AccuVote OS optical scan central count reader CC 2.0.12
- 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 4.6.1
- Election Media Processor 4.6.2

In accordance with the report of the Secretary issued on December 22, 2005, and with this subsequent reexamination, the preceding components of the Diebold System are hereby granted certification, under the following conditions:

1. Any Pennsylvania county board of elections employing TSX shall not permit the substitution of memory cards after pre-election testing. This involves careful handling and storage procedures and the use of effective seals.

2. 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.

3. 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. Future versions of TSX should be modified and incorporated so that the zero report cannot be altered through manipulation of .abo files.

2. 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.

3. 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.

4. 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 II of this report and Section III of the report of December 22, 2005, certification is being denied for the following component:

- AccuVote OS Model D optical scan precinct reader 1.96.6

IV. SUMMATION

As a result of the examination conducted on November 22, 2005, the subsequent reexamination, and after consultation with the Department's staff and consultant, certification of the **TSX electronic voting system with GEMS election management software and the AccuVote OS optical scan central count reader CC 2.0.12** 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 III 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 reader for the reasons listed in Section II of this report.**

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 with section 1105-A(a-b) of the Pennsylvania Election Code, 25 P.S. § 3031.5(a-b).

APPENDIX A



Response to Pennsylvania Request for Clarification on ABasic Issues

January 5, 2006

Overview:

This document is to address the issues raised by the State of Pennsylvania regarding the ABasic reporting scripts used by the AccuVote-TSX unit.

AccuBasic (or ABasic as it is usually called) is a tool that is used to enable the customization of reports produced by the AccuVote-TS/TSX and AccuVote-OS. The ABasic tool has controlled functionality that has only read-only access to the election and results data, and can only output data to the printer and display (in the form of a status message or prompt for Yes or No).

The ABasic scripts that are used by the AccuVote-TS/TSX and AccuVote-OS are compiled scripts and are not in a 'human' readable form. The scripts are processed by a report processor that controls what the scripts can do.

Issues:

- 1) What protection is there on the AccuVote-TSX to ensure the ABasic has not tampered with?

The ABasic on the AccuVote-TSX, along with all of the election data, is digitally signed to ensure what was downloaded has not been modified.

- 2) What mechanism with-in the AccuVote-TSX ensures the counts are zero when the zero report is printed?

The zero report is printed when the public count, the number of ballot images in the results file, is zero. Since the AccuVote-TSX only stores ballot images and not

accumulated totals, and calculates the totals by adding the votes from all of the ballots, if there are zero ballots images the sum of all the ballots images must also be zero.

- 3) What protection is there to ensure and/or validate the ABasic downloaded to the memory card is the certified version?

The GEMS user does not have permission to copy files onto the system and so cannot change the ABasic scripts installed with the certified version of GEMS.

To validate the ABasic scripts on the GEMS host an MD5 or other hash can be run to compare the files with those provided with the certified GEMS Installation disk.

- 4) What protection or detection is there against the Election/System Administrator tampering with the ABasic on the GEMS Host?

If the Election/System Administrator has the root password to the GEMS host computer they could copy an uncertified ABasic script onto the system. Note that the creation of an ABasic script requires knowledge of the ABasic scripting language, and the ABasic compiler (which is not provided with GEMS), or countless hours trying to reverse-engineer the compiled scripts.

Since the ABasic script is a read-only mechanism if any modification to the ABasic report was made that affected the printed results those printed results would not match the results uploaded to GEMS. This discrepancy would be detected during normal election canvas.

Furthermore the ballot images can be printed directly from the AccuVote-TSX for a manual verification of the results.