



Diebold Election Systems, Inc.  
P.O. Box 1019  
Allen, Tx. 75013  
  
469/ 675-8990  
Fax 214/383- 1596

Overnight:  
1253 Allen Station Pkwy  
Allen, TX 75002

March 12, 2007

Re: Response to "Voter Action Wisconsin" Complaint

Dear Mr. Kennedy:

We are replying to your February 5, 2007 letter in which you asked Diebold Election Systems, Inc. ("DESI") to respond to a Verified Complaint that a group calling itself "Voter Action Wisconsin" ("VAW") filed with the State of Wisconsin Elections Board on or about October 4, 2006. The Complaint asserts a variety of allegations about certain direct recording electronic voting systems ("DREs") that purportedly amount to violations of Chapter 5 of the Wisconsin Statutes and of Article III, Section 3 of the Wisconsin Constitution. DESI manufactures one of the DREs – the AccuVote®<sup>1</sup>-TSX DRE system with the Accuvue®<sup>2</sup> Printer Module – that is a subject of the Complaint.

As with many of the challenges that have been raised against the use of DREs, the Complaint tries to knit together various reports, studies and anecdotes in an attempt to portray the TSX<sup>3</sup> as unreliable and subject to tampering. DESI has previously and publicly responded to each of these reports or studies. In replying to your letter, we will incorporate those earlier responses. For the most part, the criticisms are based on a misunderstanding of how the system operates, a failure to appreciate the physical and procedural security in place at polling locations, or test conditions that are so divorced from how the systems are actually implemented as to make the conclusions invalid.

DESI strives to build a secure, safe and accessible voting system that meets the needs of its customers and those of the voters. We are particularly proud that we have designed systems that allow those with physical disabilities, such as vision impairment, to have the experience of voting in private and without the assistance of others. We also pride ourselves on building systems that address the particular requirements of our customers. For example, when election boards expressed a demand for voter verified paper audit trails ("VVPAT") we responded with a compact printer module that can be used with our existing line of equipment. Indeed, the Accuvue printer is used with the TSX system in Wisconsin.

Our most satisfying response, however, to the types of allegations in this Complaint is that the DESI systems have now stood the test of time and use. DESI DREs have been in use for over six years and have recorded votes in at least 23 states. Over 125,000 of our DREs are currently being used throughout the United States. And in all those years, across all those states and through thousands of local, state and federal elections, there has not been a single verified instance of a security breach. The DESI systems have also been demonstrated to be reliable. Parallel monitoring is used by many of our customers to confirm that the systems are accurately recording votes, and we have had 100% performance in all of these tests. Although there are occasional mishaps that can be avoided through better training, the predictions of organizations such as VAW have been proven to be baseless.

---

<sup>1</sup> AccuVote is a registered trademark of Diebold Election Systems, Inc. (ALL RIGHTS RESERVED)

<sup>2</sup> Accuvue is a registered trademark of Diebold Election Systems, Inc. (ALL RIGHTS RESERVED)

<sup>3</sup> This response to your letter will only address the allegations as they relate to the TSX or other DESI products.

In the attachment to this letter, we will directly address the numbered paragraphs in the Complaint, to the extent they are directed at DESI or the TSX. We will begin with Paragraph 9 because the preceding paragraphs contain general information about the complainant and Wisconsin elections. Please let me know if there is any additional information that we can provide.

Sincerely,

A handwritten signature in black ink, appearing to read "C R Owen". The signature is fluid and cursive, with the first name "Charles" and last name "Owen" clearly distinguishable.

Charles R. Owen  
Division Counsel  
Diebold Election Systems, Inc.

**RESPONSE OF DIEBOLD ELECTION SYSTEMS, INC.  
TO THE ALLEGATIONS OF VOTER ACTION WISCONSIN  
BEFORE THE STATE OF WISCONSIN ELECTIONS BOARD**

Response to Paragraph 9:

Diebold Election Systems, Inc.'s (DESI's) voting systems have proven their reliability in elections throughout the country. Additionally, several accredited, fully qualified third party testing organizations have reviewed DESI's touch screen voting systems and have approved them for use in many areas of the country.

The "study" completed by the group from Johns Hopkins was published on July 23, 2003 -- over three and 1/2 years ago. This study was conducted on limited, incomplete, draft software that was never used in any election. The resulting report was terribly flawed when it was first published, and is even less reliable now that DESI has added many additional security enhancements to its voting systems in the forty-four months since it was published.

The following security features are available in each DESI touch screen voting station, including those used in the 2006 Wisconsin election:

- Election System Touch Screen Voting Station and Election Management Software Server are Stand-Alone Devices.
  - Never connected to the Internet
  - No Networking within the Precinct (No Single Point of Failure)
- Access to the GEMS Election Management System Software application requires:
  - Physical access to the room securing the server
  - Authorized User ID
  - Authorized User Password
- Ballot styles stored on AccuVote-TSX PCMCIA memory cards are secured using digital signatures that immediately indicate tampering.
  - The PCMCIA card is secured behind a locked compartment.
  - A tumbler based key lock is used to secure the compartment.
- A Central Administrator Password with a Central Administrator Card is required to gain access to the AccuVote-TSX administrative functions.
  - The Central Administrator Password can be up to 10 digits in length and can be changed by the jurisdiction for each election.
  - The Security encryption keys can be changed for each election as well.
- A Supervisor Password with a Supervisor Card is required to gain access to the AccuVote-TSX opening and closing poll functions.

- The Supervisor Password can be up to 10 digits in length and can be changed by the jurisdiction for each election.
  - The Security encryption keys can be changed for each election as well.
- Following standard Logic and Accuracy Testing:
  - The PCMCIA card and thermal printer compartment doors are key locked.
  - The unit's security panels are closed and a tamper evident security seal is inserted to secure them and to show any signs of tampering.
- Voter Access Cards, used to initiate the voting process and retrieve the voter's ballot style, contain an encryption key that must match the key of the touch screen voting stations located within the respective precinct.
  - The Voter Access Card encryption keys can be changed by the jurisdiction for each election, further preventing the risk of card duplication.
  - If the Voter Access Card and voting station encryption keys do not match, the Voter Access Card is immediately rejected by the voting station.
- Once a ballot is cast, a voter's ballot selections are immediately encrypted, digitally signed and stored in two separate memory locations to provide redundancy.
  - Encryption keys can be changed for each election, if desired. No encryption keys are hard coded in the system.
  - Encrypted Cast Ballot Record information is stored on a secured, removable PCMCIA memory card and on internal non-volatile "flash" memory within the touch screen voting station.
  - Non-volatile memory is used to insure cast ballot information is retained, even if standard and backup power sources become inoperable.
  - The order of stored cast ballots is randomized to provide additional voter anonymity.
  - The randomization algorithm is seeded by a number of dynamic parameters, including the encryption key which the jurisdiction can change for each election.
  - Should a PCMCIA card become inoperable for some reason, cast ballot information can be securely retrieved/downloaded from the encrypted, redundant "flash" memory within the voting station.
- The integral thermal printer provides a paper-based Zero Report before the voting process begins on Election Day, confirming that no votes have yet been cast and stored by the unit. A Results Report is printed by the thermal printer, on each voting station when polls close. The paper Results Report includes all races on the ballot and the number of votes received by each candidate in each race.
- Unofficial election results can be optionally transmitted on election night to election central using the standard telephone network, not the Internet.
  - Transmitted results are secured using sophisticated Secure Socket Layer (Open SSL) encryption.

- The transmission from each voting station to election central is authenticated to validate the source of the transmission (two-way authentication).
- The GEMS Election Management Software will only accept the election results from one memory card from each voting station, eliminating the chance of record duplication.
  - Each memory card has a unique identification.
  - GEMS provides a continually updated report of the voting stations that have and have not reported results on election night.
- If a paper record of each cast ballot within a precinct or the entire jurisdiction is required, the GEMS software can print out an anonymous paper copy of each Ballot Cast Record.

Moreover, the National Software Reference Library (NSRL), which is part of the National Institute of Standards and Technology (NIST), stores a collection of software versions from many companies for a variety of applications, including election system software. File profiles are generated by NIST and posted to the NSRL from each version of the stored software, and a Reference Data Set (RDS) is created that can be used by data experts to confirm that the election software being utilized by a jurisdiction is the actual qualified and certified version of software on file with the NSRL. The RDS is a collection of digital signatures of these software applications. The NSRL contains numerous versions of DESI's election system software.

#### Response to Paragraph 10A:

The Cuyahoga County Board of Commissioners contracted with Election Science Institute (ESI) to analyze various aspects of the May 2006 Primary Election in Ohio. As DESI has repeatedly noted, and the Ohio Association of Election Officials has confirmed, the ESI study was deeply flawed in many ways.

The initial review and conclusions reached by ESI concerning the Comparison of Vote Count By Candidate were wrong. ESI conducted an incomplete analysis and failed to incorporate critical data that was provided by the Cuyahoga County Board of Elections. In fact, in some cases ESI made obvious mistakes in its own testing procedures.

There was no discrepancy between the memory cards and the Voter Verifiable Paper Audit Trail (VVPAT) totals, nor was there a mismatch between the precinct memory cards and the touch screen unit's internal memory totals. The actual vote results were balanced and verified when the Election Day administrative actions were incorporated into the analysis.

In contrast to the equipment performance, there were a number of problems with the conduct of Ohio's May 2006 primary election. Poll worker training was insufficient. These procedural issues have been corrected by the county election board administration.

ESI's review failed to take into account the procedures for handling curbside voters and 17-year old voters. As a result, the report erroneously concluded that precinct totals from specific precinct or voting center memory cards did not match the totals from the touch screen unit's internal memory located on the unit's motherboard. Cuyahoga County used paper ballots for these special voting cases. The votes were inputted into touch screen units and the totals were placed on separate memory cards. It is apparent that ESI tabulated the memory card totals from the touch screen units used within the precinct for walk-in 18 year and older voters, but did not include the totals from the memory cards for curbside voters or 17-year old voters. This omission caused the variance between the two totals. The Cuyahoga County Board of Elections notified ESI of this omission prior to the final report being issued, but ESI neglected to make the corrections prior to releasing their final report.

Some of ESI's own testing procedures were flawed. On several memory cards that were uploaded by ESI from the touch screen unit's internal memory and used for the ESI analysis, zero votes were present; however, the internal memory of the touch screen units contained between 30 and 50+ votes, respectively. The original memory cards used in these touch screen units during the actual election contained the same number of votes as the internal memory of these units. ESI operator error appears to be the cause of these memory cards used in the ESI analysis not containing any votes, as they should have been uploaded directly from the touch screen's internal memory, which did contain the correct number of votes cast. ESI does state in the analysis that "Human error can not be ruled out as the source of the discrepancies reported."

The accuracy and reliability of DESI's system has been tested by federal and independent laboratories, and has passed a regime of stringent parallel monitoring accuracy tests. US District Judge Daniel Polster stated, "Given the recent history of elections in this county, the Court believes the Cuyahoga County Board of Elections did an excellent job conducting today's election."

The Ohio Association of Election Officials was very concerned about the misinformation included in the ESI study and published a press release on August 23, 2006, in which its president said, "As we had stated previously, the audit in Cuyahoga County provided no reason for voters to question the integrity of their elections process or the machines that record their votes." He continued, "Those of us who do this for a living knew immediately that something was wrong with the study, and it disheartened us that so many people used it as an excuse to try and erode the public's trust in our elections system." Jeff Matthews, past president of the OAEO, criticized ESI for the "poor execution" of its audit. "Unfortunately, ESI either didn't know how Ohio's elections systems worked, or chose to ignore their own people who tried to advise them of it. Their methodology was flawed, their execution was poor, and their results and conclusions suffered as a result. The real losers of this non-accredited agency's debacle

are the voters of Ohio who were given false conclusions and made to believe that their elections are unsafe.”

The OAEO recognized that claims that vote totals on memory cards did not match vote totals on paper trails were found to be untrue. No votes were lost.

Response to Paragraph 10B:

Several accredited, fully-qualified third party testing organizations have reviewed DESI’s touch screen voting system and have approved it for use in many areas of the country. The “study” conducted by a professor and two students at Princeton identified in Paragraph 10B, on the other hand, is unscientific and unreliable.

Their study did not undergo a quality peer review, and failed to consider many pertinent facts. The individuals generating the report would not disclose where or how the unit was acquired. The AccuVote-TS Ballot Station software analyzed (version 4.3.15) is, in fact, a full two generations behind the current version and does not include many of the security enhancements that the latest generations provide. This software was not used in *any* jurisdiction during the November 2006 election. The report’s conclusions are, not surprisingly, erroneous. The layered protection offered by the AccuVote-TS unit combined with the physical security and chain-of-custody procedures associated with elections are sufficient to ensure that all votes are accurately recorded and tabulated.

Also, while this study asserts that memory cards can somehow propagate a virus, it fails to take into account that the memory cards can be examined for extraneous files that should not be present and for the actual install file that should be on the card. That same file can be “hashed” to compare with the hash codes archived on NIST’s National Software Reference Library.

Moreover, the Ballot Station software includes enhanced security features such as:

- Advanced Encryption Standard (AES) election result data encryption;
- Digitally Signed memory card data;
- Dynamic system passwords; and
- Secure Socket Layer data encryption for optional transmission of unofficial election results.

Response to Paragraphs 11-12D:

These paragraphs are not directed at DESI.

Response to Paragraph 12E:

Contrary to the assertions in this paragraph, the touch screen tabulation system used in Maryland jurisdictions beginning in November 2002 performed extremely well

during the 2006 elections. In fact, when the DESI touch screen systems were installed virtually state-wide, Maryland experienced a 40% reduction in voter error when 2004 presidential election statistics were compared to the 2000 presidential election statistics. Maryland had the most accurate voting system in the entire country, with a residual vote count of 0.30%.

The ExpressPoll electronic poll book, a separate system from the touch screen tabulation units, was first used during the Maryland September 2006 primary election. A last-minute change requested by the state involving two instructions screens and a hardware-related networking item caused certain voting units to undergo a one-minute re-boot. No voter information was lost during the validation process.

If “one voter” were actually locked out of a voting unit, that voter could have voted on a provisional ballot. A post-election canvass would determine if that voter had actually cast an electronic ballot, and thus whether the board of elections should look to that voter’s provisional ballot.

The issues discovered during the primary were rapidly identified and eliminated before the ExpressPoll units were used in Maryland’s November 2006 general election. The 5,500 ExpressPoll units used during the general election were received with tremendous acceptance by voters and election officials. A total of 1,610,655 voter access cards were processed and 29,481 provisional ballots were also processed. One of the ExpressPoll units processed 1,207 voters, or one voter every 38 seconds, which evidences phenomenal system performance.

DESI was not responsible for the actual distribution of election materials to the polling locations in Maryland. During the Maryland September 2006 primary election, election officials in Montgomery County failed to include the touch screen voter access cards in the election supply bags that were delivered to each voting location. This caused a delay in the voting process in Montgomery County. This was human error that is perfectly analogous to an election official forgetting to include paper ballots, and had nothing to do with the performance of the voting technology. Once the Voter Access Cards were delivered to the precincts, voting proceeded as usual.

Similarly, the allegation that memory cards were left in voting machines in certain precincts after tabulation is a procedural issue that has nothing to do with the performance of the system. All election results are encrypted and the memory cards are digitally signed to indicate any attempt to tamper with the data on the memory cards. In addition, a report within the GEMS election management tabulation software indicates which voting machines have uploaded election results and which ones have not. It is a simple process to determine which memory cards have not been uploaded.

The changing, and sometimes conflicting, political views of former-Governor Ehrlich are readily available in various print and online publications.



Finally, the State of Maryland requires approximately 600 temporary Election Support Staff to handle various basic tasks on Election Day. DESI uses an outside hiring agency to ensure that the State is provided with sufficient Election Support Staff. While the State requires a background check to be run for certain election-related positions, particularly those positions with access to the workings of the elections systems, it does not require background checks for Election Support Staff. Accordingly, despite any report that appeared in the Washington Post, DESI fully complied with Maryland law when having a hiring agency provide temporary Election Support Staff without running background checks.

Response to Paragraph 13:

Please see DESI's response to Paragraph 10B above.

Response to Paragraph 14:

Despite the various assertions of "security flaws," there have been no validated instances of security breaches of DESI's voting systems. Indeed, states that routinely post results of parallel monitoring from actual elections have seen 100% accuracy. See, for example:

[http://www.ss.ca.gov/elections/voting\\_systems/2006\\_nov\\_pmp\\_findings\\_final\\_rpt.pdf](http://www.ss.ca.gov/elections/voting_systems/2006_nov_pmp_findings_final_rpt.pdf)

[http://www.ss.ca.gov/elections/voting\\_systems/2005\\_pmp\\_report\\_final.pdf](http://www.ss.ca.gov/elections/voting_systems/2005_pmp_report_final.pdf)

[http://www.ss.ca.gov/elections/voting\\_systems/november2004\\_pmp\\_report.pdf](http://www.ss.ca.gov/elections/voting_systems/november2004_pmp_report.pdf)

[http://www.ss.ca.gov/elections/voting\\_systems/march\\_2004\\_pmp\\_report.pdf](http://www.ss.ca.gov/elections/voting_systems/march_2004_pmp_report.pdf)

[http://www.ss.ca.gov/executive/press\\_releases/2006/06\\_002.pdf](http://www.ss.ca.gov/executive/press_releases/2006/06_002.pdf)

<http://www.aapd-dc.org/dvpmain/paperballot/elecvote.html>

Response to Paragraph 14A:

Polling locations have instituted physical security and monitoring long before the invention of electronic voting. Those procedures can and should be adopted to the newer equipment. Voting units are used in an environment where there are procedures to monitor the equipment while in storage and in use. There are also tamper-evident devices that can detect whether any tampering has occurred. Voting units could be produced with locks and exteriors as robust as ATMs, but the cost of each voting unit would rise significantly and may no longer be economically feasible. Because ATMs, unlike ballot stations, are not always under the watchful eyes of bank workers, they are designed to withstand harsh attacks that would otherwise attract the attention of bystanders. Election systems, on the other hand, are used in an environment occupied by poll workers and other voters.

Response to Paragraphs 14B-D:

If tamper-evident tape were used on the door covering the memory card on this device, then any tampering can be detected. If tamper-evident devices were actually taken into account, as Mr. Felten claims, then tampering would have been evident regardless of the software he installed on the unit.

Response to Paragraph 15:

The fact that special interest groups file litigation is certainly no indication that their allegations have merit. No court has required any change to DESI election systems, nor has any court interfered with a relevant voting board's exercise of its expertise and discretion in choosing or buying DESI's voting systems.

Response to Paragraph 16:

A number of third-party testing organizations have reviewed and approved DESI's voting systems for use. DESI continually assesses security concerns and updates its systems when warranted.

Response to Paragraph 16A:

DESI has always been willing to enhance the security of its system when presented with a valid study from a reputable authority that has examined DESI's equipment. Due to the subjectivity of any security assessment, however, DESI does not necessarily agree with all of the findings of the assessing authority, particularly because they may not have considered factors of which they were unaware or did not recognize.

All security items are not high risk and do not have a high impact on a voting system. Claims by individuals who report the total number of issues in a report without taking the nature of the risk or impact into consideration are not working in anyone's best interests.

Response to Paragraphs 16B-C:

Notably, the election authorities in Ohio and Maryland have been satisfied that the cited studies were either overblown or that DESI has responded to the concerns. In Maryland, a trial court judge held an evidentiary hearing and concluded that the DESI systems could be used in elections despite plaintiffs' allegations about the RABA report.

Response to Paragraph 17:

This paragraph is not directed at DESI.

Response to Paragraph 18:

This paragraph is not directed at DESI.

Response to Paragraph 19:

The Complainant does not and cannot offer any specifics to support his claim that DREs are particularly susceptible to human error. DREs have been used successfully throughout the country, and exit polls demonstrate that voters are quite pleased with their ease of use. With any new technology, there is a learning curve before voters and poll workers become familiar with even the most intuitive device. There were undoubtedly learning curves when lever machines and punch cards were introduced.

Response to Paragraph 20:

DESI's voter verifiable paper audit trail (VVPAT) solution, the AccuView Printer Module, contains a unique internal compartment that secures the paper trail of votes cast. This system does not allow poll workers to view previously-cast audit records when the exterior cover of the VVPAT is opened, because the paper that contains the voter selections is located within an inner compartment that is secured with a tamper-evident security device. This inner compartment protects the integrity of audit record information. A ratcheting device in the design prevents the paper from being pulled from the inner compartment. This further increases the integrity of the DESI VVPAT unit. This additional layer of security and privacy protection eliminates the possibility of someone lifting the exterior cover of the VVPAT unit to view previous voters' selections. While the reel-to-reel VVPAT design appears to be the standard for the vast majority of election system manufacturers, DESI believes the security provided by the VVPAT inner compartment is essential to meet the privacy and integrity standards expected by voters.

The DESI VVPAT printer also includes a unique magnification panel to enlarge printed text for voters with vision impairment.

DESI is also the only election system supplier to provide a VVPAT privacy cover which enables blind voters to vote in complete privacy, meeting Help America Vote Act privacy requirements.

Response to Paragraph 21:

This paragraph is not directed at DESI.

Response to Paragraph 21A:

The voter does, in fact, have a method through the VVPAT record and county audit procedures to ensure that his or her ballot was recorded correctly. The purpose of

the VVPAT record is to address any discrepancies in the electronic ballot. The VVPAT by its nature is a voter verifiable record of the voter's selections.

Response to Paragraph 21B:

DESI uses thermal paper that is of sufficient quality to retain its information to be used for multiple audits and recounts and, when stored properly, meets and exceeds the period of retention required by federal and state standards.

There are many different grades of quality in the thermal papers and coatings available on the market. The thermal paper used in DESI's DREs is of a much higher quality than the type used for receipts in the average retail store. The text printed on thermal paper used in DESI's DREs can last at least five years, and studies have found that this paper can retain text longer than paper containing text produced by inked ribbons.

Any paper is susceptible to changes when exposed to heat, even paper that has been printed with ink. Regardless, the storage and handling requirements for the paper used in voting terminals should not require them, after they are printed, to be exposed to sunlight or extremes of heat.

Response to Paragraph 22:

This paragraph is not directed at DESI.

Response to Paragraph 22A:

Whether a lock is sufficiently robust is a subjective determination that must consider where and how the lock will be used. DESI believes that the locks on its DREs are appropriate for this application.

Response to Paragraph 23:

This paragraph is not directed at DESI.

Response to Paragraph 23A:

If tamper evident devices were used on this device for the door covering the memory card, then tampering would have been detected.

If tamper evident devices were taken into account, then regardless of the software installed on the unit, tampering would have been evident.

In addition to tamper evidence, parallel monitoring can be performed on Election Day in an effort to catch malfunctions or malicious code that might only be in effect on

the day of the election. Parallel monitoring is effective as it emulates voting activity that would occur throughout the day on voting terminals that are pulled at random from randomly selected vote centers.

Response to Paragraph 24:

This paragraph is not directed at DESI.

Response to Paragraph 24A:

Please see DESI's response to Paragraph 10A above.

Response to Paragraph 24B:

Please see DESI's response to Paragraph 21A above.

Response to Paragraph 24C:

Manual audits are usually conducted on a sample number of precincts in a county. If the individual's claim is taken further, then no system could ever meet the law except through manually counting paper ballots. Not even optical scan devices would satisfy the claim as there is no evidence given to the voter that his optical scan ballot has been counted correctly by an optical scan device. The only indication usually given to the voter is that her ballot has been cast by incrementing a ballot cast counter on the optical scan device. The ballot cast counter is also available on the DRE device.