

March 2, 2006

~~REDACTED~~  
Producer  
ABC News  
1717 DeSales Street  
Washington D.C. 20036

~~REDACTED~~  
ABC News has sent certified letters to several Diebold Election Systems and Diebold, Incorporated employees involving a number of issues related to electronic voting. We want to directly respond to the allegations contained in each of those letters in a detailed fashion in order to strongly and precisely clarify our position.

- Diebold was contracted by Maryland and Georgia to participate and provide support for the 2002 and 2004 elections. This was especially important as the 2002 election was the first use of the touch-screen system in both states. All Diebold activities were supervised by state and/or county election officials, adhering to applicable election laws within each state. In particular, you mention our presence in Montgomery County. The supervision provided in areas within Montgomery County, such as the computer/tabulation room, is well documented by the county.
- The operating system upgrade installed on the Georgia machines for the November 2002 election involved only the operating system, Windows CE, and had nothing to do with the Diebold firmware loaded onto the machines. The Diebold touch-screen firmware version used in Georgia was indeed certified by the National Association of State Election Directors (NASED) in March of 2002 (NASED control number 010702-4.1.11). The Federal Election Commission ITA lab did, in fact, review that the operating system upgrade applied to the Georgia machines was not affecting anything other than the underlying Windows CE operating system and satisfactorily communicated such to the Georgia Secretary of State well in advance of the November 2002 election. In addition, following the inclusion of this operating system upgrade, each touch screen voting machine was subjected to logic and accuracy testing by the jurisdiction before it was deployed for the election, verifying its accuracy and operation. Your source's comments about the software being malicious are absurd and misguided. Furthermore, everything done to the system in preparation for the election was done with the full consent, cooperation and oversight of the State of Georgia and Kennesaw State University. Allegations to the contrary are a misrepresentation of the truth.

- Election officials run the election process. Diebold Election Systems provides the voting equipment used by the jurisdictions and will provide supervised service support if requested by the jurisdiction.
- Diebold Election Systems' software has been escrowed for many states throughout the country, including Maryland and Georgia. The software is normally placed in escrow with an independent third-party organization, and is available to the state under a non-disclosure agreement if they so choose.
- Diebold does not develop election procedures for states. Each state establishes its own election procedures based on their respective election laws.
- States, especially Maryland and Georgia, should feel very confident using Diebold's voting systems for a number of reasons: 1) The system, including source code, has been fully reviewed by the Federal Election Commission and their Independent Testing Authorities, 2) independent testing organizations such as SAIC and others have reviewed Diebold's touch-screen system and approved its use for elections, 3) the states of Maryland and Georgia have conducted "real life" Parallel Monitoring accuracy tests of the equipment which proved it to be 100 percent accurate, 4) prior to every election every voting unit is subjected to logic and accuracy testing performed by the jurisdiction before it is deployed for use on election day, and 5) a Carl Vinson study conducted following the initial use of the statewide touch-screen system deployment in Georgia indicated 98% of all the voters surveyed indicated they had absolutely no difficulty using the system, and voter confidence in Georgia increased a very significant 17%. A recent InfoSENTRY survey published February 4, 2006, indicated, "Americans have higher trust in the confidentiality and accuracy of computerized voting systems, commonly known as Direct Record Electronic (DRE) and "touchscreen" systems, than in other voting technologies being widely considered as states and counties rush to comply with the Help America Vote Act (HAVA) of 2002."
- Jurisdictions running Diebold election system software can compare the software used for their election with a digital fingerprint of the very software that was qualified/certified for use within the state to verify it is exactly the same software and no alterations have been made. The National Institute of Standards and Technology (NIST) has developed the National Software Reference Library (NSRL), within which digital fingerprints of Diebold's election system software are stored and available for verification purposes by jurisdictions.
- In your letter, you mention a "back door" to the GEMS election management system. There is no "back door" to the GEMS system. What Metamor discovered was that if the server is not properly physically secured (as is the procedure in election offices nationwide), and if "no" passwords are used to protect the system, that a malicious person could gain access to the database. This is true of any type of voting system with a database. Once again, if proper procedures are not implemented and followed, even the national missile defense system is vulnerable. It is strongly recommended by Diebold that election offices use the GEMS server as a dedicated server, solely for election purposes. The server should contain no ancillary software programs that are not necessary to run the election. There is no risk of malicious tampering if basic procedures such as passwords are implemented. Again, several third party security organizations have thoroughly reviewed the Diebold system and have approved it for use in elections.

- In regards to memory cards, again, security processes and protocols need to be followed for any mission-critical operation. Several security tests, including recent testing by the University of California at Berkeley, and an FEC Independent Testing Authority found Diebold voting machines to be accurate and secure when following the necessary steps for security. Unsubstantiated accusations are easy to make, but proof of the allegation leads to different outcomes. Case in point, an activist group brought Harri Hursti to Leon County, Fla., where the supervisor of elections gave Hursti full unfettered access to his voting system (not an acceptable practice by Florida election standards or the county's own policies and procedures). Hursti made claims he could "hack" the Diebold optical scan system (not to be confused with the precinct-based touch-screen system used in Maryland or Georgia). Upon inviting Hursti to California to prove his theory, the demonstration was cancelled by Hursti, as he informed the Secretary of State's office he could not successfully accomplish his claims if standard election procedures were followed.
- Your letter indicates that a leading computer scientist claims the voter smart cards can easily be altered and inserted into the machines to change votes. This is blatantly false, misleading information. Your source is obviously not aware of the well publicized fact that our voter access cards contain an encryption key that protects them from duplication. This encryption key is dynamic and can be changed for each election, providing excellent security protection. Advanced data security professionals that have thoroughly reviewed the system and understand its functionality agree the voter access cards are very secure.
- The touch screen election results stored on memory cards locked into the side of the voting station are secured using sophisticated 128 bit Advanced Encryption Standard data encryption, and are digitally signed to indicate any tamper attempt. Also, to clarify a potential misunderstanding, the memory cards used in the touch screen units used throughout Maryland and Georgia are not the same design and do not store election results in the same manner as the optical scan units.

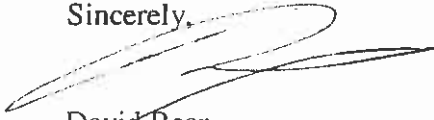
As you may be aware, there are a select number of vocal activists that would prefer to revert back to full paper ballots in place of using touch-screen voting system technology. Diebold does offer a touch screen voting station with a voter verifiable paper audit trail (VVPAT) printer that has been successfully used in several states during the past year. Approximately two years ago, we demonstrated a prototype of a VVPAT for the AccuVote-TS touch screen voting stations used in Maryland. At this time, Maryland has not developed standards of functionality for the VVPAT, nor have they mandated the use of the VVPAT printer with the units.

Also, the Cal Tech/MIT Voting Technology Project, titled "Residual Vote in the 2004 Election", clearly indicates that Maryland had the most accurate voting system in the country during the 2004 general election. This report can be found at [http://www.vote.caltech.edu/media/documents/vtp\\_wp21v2.3.pdf](http://www.vote.caltech.edu/media/documents/vtp_wp21v2.3.pdf).

In closing, Diebold Election Systems feels it has clarified in detail the allegations directed against our company, mostly by what appears to be a misinformed, disgruntled ex-contractor. The accuracy of our system is proven by the many tests and studies that have been conducted over the past three years. Also, I believe Mr. Jacobsen indicated in his interview with you in mid-December that he is not the designated spokesperson for Diebold Election Systems. It's

unfortunate that the official spokesperson for Diebold Election Systems was not contacted to respond to these questions, as more complete answers could have been provided at that time. Should you feel the need for further clarification, please do not hesitate to contact me directly.

Sincerely,

A handwritten signature in black ink, appearing to read "David Bear", written over the word "Sincerely,".

David Bear  
Media Liaison, Diebold Election Systems

Cc: Mark Radke  
Diebold Election Systems, Inc.

Mike Jacobsen  
Diebold, Incorporated