

From: Black Box Voting, Inc.
Date: Sept. 7, 2005
Reply to: Bev Harris – 330 SW 43rd St Suite K PMB 547 Renton WA 98055
425-793-1030 bev@blackboxvoting.org

Public Records Request # 090705a

We are requesting the public records. Please e-mail bev@blackboxvoting.org with estimated price and to whom we should send the check, and the address to send it to. /

Records requested:

1) All correspondence, documents, notes, memos, e-mails etc. pertaining to the July 4, 2005 Black Box Voting Security Alert written by Harri Hursti, and/or pertaining to the Diebold optical scan "hack" or security test performed in Leon County, Florida by Black Box Voting, Harri Hursti et. al. Please include:

Any directives, suggestions, explanations, answers or advice from Diebold Election Systems Inc. pertaining to this report or the above referenced Leon County testing.

2) Please provide any document or e-mail containing the name Hursti dated May 2, 2005 until the date of your receipt of this request.

3) Please provide any document or e-mail containing the name Black Box Voting or Bev Harris dated May 2, 2005 until the date of your receipt of this request.

4) Please provide any document or e-mail pertaining to memory cards, dated May 2, 2005 until the date of your receipt of this request.

Thank you.

Bev Harris
Director
Black Box Voting, Inc.

Copies of 1 FAX AND 1 LETTER, both from the Secretary of State's Office. No other documents or email with names per request.

*Thomas W. Schellum
Elections Officer
Cochise County, Arizona*



JAN BREWER
SECRETARY OF STATE
STATE OF ARIZONA

PRESS RELEASE

For Immediate Release

August 26, 2005

For more information, contact Kevin Tyne at (602) 542-0681

Secretary of State Brewer Calls for Additional Security Election Practices
Arizona Among Nation's Leaders in Security Measures for Voting Systems and Procedures

PHOENIX – Secretary of State Jan Brewer announced today additional detailed procedures concerning election security. The new procedures are an extension of the Brewer Voting Action Plan, which is a comprehensive study and recommendations released earlier this year focusing on election technology, policies, procedures, and security.

"The public's awareness of election security issues is still high and has remained high since the 2000 elections. Our actions and careful deliberations should make the citizens of Arizona feel secure in our elections," Secretary Brewer said.

The specific new procedures that the Secretary of State's office will work to implement include:

- Insuring that no single person is in charge of election setup, programming, card burning, tallying and reporting
- Increasing security procedures around the handling and programming of voting machines so that two election officials must sign off on all card swaps or removals
- Specifically identifying all memory cards so that a card from another source is easily identifiable
- Sealing memory cards in voting devices until the machine is returned to election central
- Improving security around the transportation of memory cards
- Improving software auditing procedures for election management computers
- Reconciliation of canvass reports from the election management system against the paper tape totals generated at the polls
- Increasing penalties for tampering with election equipment or software

Arizona is one of only a handful of states in the nation to have conducted a large-scale analysis of its own current voting technologies, certification procedures and general standards and operating procedures for administering federal and state elections.

"The development of these important procedures prior to the elections in 2006 is part of my ongoing commitment to ensure integrity in our election process. With voting technology changing, it is imperative that Arizona be proactive in developing comprehensive procedures that ensure the security and integrity of our elections. I look forward to working with interested groups, legislators, and county and local election officials in implementing these procedures," stated Secretary Brewer.

Added Brewer, "All Arizona election officials recognize the need for securing against potential vulnerabilities in order to maintain the integrity of our overall elections; I remain extremely confident in the proactive approach our state has taken to secure our election process."

DIEBOLD

Diebold Election Systems, Inc.
1611 Walnut Street
Akron, OH 44316
972 342-6026
fax 972 342-6026
email: sales@diebold.com

RECEIVED
SECRETARY OF STATE
2005 AUG 25 AM 10:47

STIVE MORELAND
Director of Election Services

August 23, 2005

Honorable Janice K. Brewer
Secretary of State
1700 W. Washington Street
7th Floor
Phoenix, Arizona 85007-2888

Dear Secretary Brewer:

Thank you for your letter dated August 11, 2005. I appreciate the opportunity to address any security concerns with our voting system.

The Diebold Accuvote Optical Scan Voting System, and its predecessor Global Elections Systems Optical Scan (OS) Voting System, have been in use for over 10 years in hundreds of counties throughout the country without a single security breach having ever occurred.

In response to your letter dated August 11, 2005 I want to first address the claims made in the BBV report. The report claims to have been able to alter the election results in two ways. The first claim purports to have been able to add additional votes to an individual candidate's vote total. In fact, what they changed were the votes stored in the data tables, not on the memory cards. At no point in this process were votes "lost" or "altered". The GEMS system contains a feature whereby an election official can manually enter the election results for a polling place. This feature, titled Manual Entry, is present in the event that the AccuVote-OS memory card at a remote polling place is not able to be uploaded or driven in to the election headquarters. As you may recall, Apache County had to use Manual Entry in the November 2004 Presidential Election in order to be able to report its election results in a timely manner. Without Manual Entry the County may have been significantly delayed in reporting its election results. The feature is a tool designed to assist election officials, and is not a security vulnerability.

The GEMS program utilizes the Microsoft (MS) Access database engine. In the past BBV has claimed that anyone with access to the GEMS server could manipulate data through MS Access to change election results. There are several incorrect assumptions in this misleading statement.

1. This preposterous claim assumes that the computer operator has unsupervised access to the GEMS server computer and knows all of the passwords. The GEMS server computer should always be in a secure location with access granted only to authorized personnel and adhere to proper password policies.

2. The claim also assumes that the GEMS server would have MS Access loaded on it. In fact, Diebold does not load MS Access onto a GEMS server and recommends counties to keep MS Access off the server. To my knowledge, no Counties in Arizona have MS Access on their servers.
3. Lastly, the claim assumes that there is no canvass procedure which would catch an inconsistency in vote totals.

The second claim purports the ability to alter an optical scan memory card. The only portion of the memory card that can be accessed contains written text which appears on the printed tapes. The actual votes could not be accessed or modified. Further, the AccuVote-OS memory card does not make use of a machine-executable program stored, and implements no ability to execute any programs from a memory card. The system includes no provision for modification of vote results by an external program.

For your information, I have attached a memorandum from Georgia Director of Elections, Kathy Rogers, which has been distributed to the counties within Georgia in direct response to the same BBV allegations. The State of Georgia is a current customer of DESI's Voting System.

As you have indicated, proper procedures designed to limit access to sensitive election information along with proper canvassing procedures are essential to maintaining the security and integrity of Arizona's election systems.

The procedures that you have outlined in the Brewer Voting Action Plan are very positive steps to ensuring the integrity of your system and we commend you for proposing them. Should you need further assistance in this important matter, our company is available to work with your staff for further procedural assistance or answer any questions you might have.

Please let me know if we can be of any further assistance. Diebold Election Systems looks forward to working with you and your staff to ensure the security and accuracy of Arizona's elections.

Sincerely,



Steve Moreland
Senior Director, Customer Service
Diebold Election Systems

Encl.

RECEIVED
SECRETARY OF STATE
2005 AUG 25 AM 10:47

Black Box Voting Optical Scan Test - Response

First of all, certain activists recently did some so-called "testing" in Leon County. This testing was inherently flawed because the local election supervisor 1) allowed unauthorized people physical access into the GEMS server room, 2) provided them with unrestricted access to the server using his "secret" passwords, and 3) enabled the activist to use the system with no restrictive supervision. None of these scenarios are realistic, and the blatant disregard by this supervisor for proper physical and electronic security standards makes claims associated with this "testing" unrealistic.

There is **NO EXECUTABLE PROGRAM** stored on the optical scan memory card. Claims made to the contrary by activists are incorrect. Votes stored on the memory card can not be changed in any way by anything stored on the memory card. Inaccurate statements concerning an executable program allegedly able to manipulate the vote totals are being presented by certain activists in an attempt to falsely downgrade the security of the Diebold optical scan solution. The data in question on the memory card provides a simple print template for the local optical scan printer and nothing more. No vote totals, either those stored locally or those transmitted to election central, can be altered using this printer template.

As any election official is aware, the overall integrity of an election is comprised of reliable equipment, adequate procedures and people. The activist claims state that the printout of the optical scan unit can be changed to cause confusion following an election. As previously discussed, there is no executable program on the memory card and the activists, with full access to the system, could not modify the election results on the memory card. Changes to the printer template that would cause incorrect information to be printed would be immediately recognized during pre-election logic & accuracy testing of the unit. As any election official is aware, once logic and accuracy testing is successfully completed on a unit its memory card is secured in the optical scan unit using a tamper-evident security audit tag. Therefore any attempt to remove the memory card in order to modify it in any way would be immediately recognized.

As in many previous accusations, electronic election system activists alter the truth to support their position, and do not take into consideration the layers of security provided by the equipment, procedures and people associated with the election process.

RECEIVED
SECRETARY OF STATE
2005 AUG 25 AM 10:47



Secretary of State
Elections Division
2 Martin Luther King, Jr. Drive
1104 West Tower
Atlanta, Georgia 30334

Cathy Cox
SECRETARY OF STATE

KATHY A. ROGERS
DIRECTOR
(404) 658-2871
FAX (404) 651-8531
krogers@sos.state.ga.us

August 17, 2005

MEMORANDUM

TO: Election Officials
FROM: Kathy Rogers, Director
RE: Mailing from Black Box Voting

Recently many of you received a document from Black Box Voting describing an alleged security issue with the Diebold Accuvote Optical Scan Tabulators. As promised in an earlier email, the purpose of this letter is to provide you with the actual facts regarding this alleged security breach.

The election supervisor in Leon County, Florida unfortunately allowed unauthorized Black Box Voting activists full and unrestricted access to his GEMS server, and provided his "secret" passwords. As you are well aware, this type of unrestricted access and the blatant disregard by this supervisor for proper physical and electronic security standards makes all reported claims and findings of these activists unrealistic in a true elections environment. As I am sure you would agree, unrestricted and uncontrolled access by members of the general public to ANY election management and tabulation system – including mechanical and paper-based systems – could result in a serious compromise of the accuracy and legitimacy of any real-world election. That is why all responsible election officials, in Georgia and elsewhere, have clear security protocols and standards for access to the voting and tabulation equipment.

If you have read the report, you will note that it purports to have been able to alter the system in two ways. First, the activists claim to have been able to add additional votes to an individual candidate's vote total. In truth, what was changed were votes in the data tables within GEMS. They did not alter the votes on the memory card, nor the internal results of the archived files. Changing the vote totals in these data tables can be compared to allowing someone access to an electronic Excel spreadsheet of vote totals and then saying "now see if you can change these results." What the activists did not report to you is the fact that in a real world election environment none of the votes added into the

Memorandum to Election Officials

August 17, 2005

Page 2

data tables would actually match the memory cards created by the database nor the tapes printed by those cards. These vote totals would also never reconcile with the DRE recaps which are completed at the polling place. As is so often the case, critics of our system choose to completely ignore the overlapping and redundant security safeguards – including tapes printed from each voting terminal – which exist precisely to prevent the sort of results manipulation they sought to demonstrate. While an election official should never allow complete and unauthorized access to a GEMS server, even if this did occur, it would be quickly and easily discernable upon a quick audit of the results.

The second claim made by the activists was the ability to alter an optical scan memory card. In truth, the only portion of the memory card which was accessed was the portion of the card which records written text that appears on the printed tapes. The actual votes could not be accessed nor could they be altered or manipulated. In fact, there is not an executable program stored on the memory card which would even allow such an attack to occur. What the report does not tell you is that the activists would not have been able to load the memory card on which they had altered the text back into the GEMS server. As you know, the server will not recognize any memory card which has been changed or revised once it has been downloaded for an election. Even if someone did gain access to your server and then changed the text which appears on the printed tapes, this breach of security would be easily identified during Logic and Accuracy testing.

For your review, I have enclosed a copy of a letter Diebold sent to the Leon County elections supervisor which details the seriousness of allowing unauthorized access to his GEMS server. One statement within this letter accurately sums up the actions of this election supervisor “Your improper actions are equivalent to leaving your car unlocked, with the windows down and keys left in the ignition and then acting surprised when your car is stolen or vandalized.” It is also extremely ironic that the stated agenda of many of these activists is the elimination of any electronic voting or tabulation device and a return to hand-marked, hand-counted paper ballots. Imagine a “test” analogous to the one conducted in Leon County in which outsiders were permitted unrestricted access to a room full of voted paper ballots – which could be easily destroyed, re-marked, stolen or replaced at will. And in that scenario, the fraud would likely be undetectable, since manual paper ballot systems lack the overlapping checks and balances that are the hallmark of our current voting system. I urge you to read Diebold’s letter carefully as it reinforces the fact that basic security procedures are the foundation of any election system and that to allow someone to purposely breach that security is an unconscionable act that calls into question the integrity of the entire elections process.

All Georgia election officials recognize that carefully designed professional testing of our election platform – including a search for any potential vulnerabilities – is essential to maintaining the integrity of our elections process. It is for just that reason that in Georgia

Memorandum to Election Officials

August 17, 2005

Page 3

we have such an extensive testing regimen -- beginning with national certification testing and continuing with state certification testing, acceptance testing of all system components, and logic and accuracy testing prior to each election.

If you have any questions or concerns, please do not hesitate to call me or one of the staff members at the Center for Election Systems at KSU. Thank you for the job that you do and for your dedication to ensuring that Georgia Elections are conducted in a secure environment!

KR:pgf

Attachment

- From Black Box Voting Document Archive -