GlobalResearch
Center for Research on Globalization

The Two Faces of Diebold

By Rebecca Abrahams
Global Research, June 28, 2007
Huffington Post 2 November 2006

Region: USA
In-depth Report: Election Fraud in America

Stunning Document Surfaces to Show That America's #1 Voting Machine Manufacturer Hides Security and Operation Flaws from The State of Maryland and the Country

In September, 2003 Linda Lamone, the Administrator of Maryland's State Board of Elections and President of the National Association of State Election Directors (NASED) hands over a critical study on the security of the Diebold Election Systems machines that count all of Maryland's votes.

Between the time that the State of Maryland commissioned the highly respected Scientific Applications International Corporation (SAIC) to evaluate the effectiveness and security of their electronic voting machines and the time that the study is made public, critical pieces of information have been edited, omitted and, in some cases words added, to fundamentally alter the original meaning of the report's conclusions.

Enter the world of electronic voting machines, the "cure" to hanging and dimpled chad.

It is a seamy world of secrecy, proprietary software, partisan executives "committed to helping Ohio deliver its electoral votes to the President", politicians asking programmers to design software to flip vote totals, and lots and lots of money.

And it is a world of completely inconsistent realities. Diebold and the other manufacturers insist that their machines are safe and secure yet every single cyber security expert and computer scientist has, for years, been screaming into an empty wilderness of media attention, that . . .

The machines can be hacked, by the implanting of malicious code, at the factory.

The machines can be hacked during transport from the factory.

The machines can be hacked while on "Sleepovers" before the election.

The machines can be hacked (in 1 minute with a .50cent mini bar key) during the election, and

These machines can be hacked, at the tabulator, after the election.

What makes this SAIC report, called "The Pentagon Papers of Electronic Voting" by some computer experts, so important is that:

1. It shows, in black and white, that what Diebold says to election officials and voters across the country is not the truth.

2. It shows that there are virtually no security protocols in place for certain Diebold machines and that the recommended security protocols were purposely removed.

3. It shows that the analyzed Diebold machines were not functional nor secure for use in elections and raises serious doubts that they are ready for the November 7, 2006 Midterm elections.

The study, dated September 17, 2003, is the response to research performed by Johns Hopkins University Computer Science Professor Avi Rubin citing severe security flaws on the Diebold touch screen machines, including a surprising lack of security, (encryption), on the memory cards. Maryland sought to ascertain whether their Diebold Touch Screen machines were, in fact, safe for Maryland voters to use.

But Diebold, in return for allowing their super secret, proprietary machines to be examined by the independent laboratory, insisted on two huge concessions from the State of Maryland.

First, SAIC would not be allowed to even look at the source code, the heart and guts of electronic voting machines. Second, they would be allowed to go through the SAIC Report, line by line, and redact anything and everything that they felt was proprietary, had a potential for security breaches or could provide a roadmap for anyone who wanted to compromise the system.

In other words, whatever they wanted to do with the public part of the report they could.

In addition to its value in showing the massive difference between the public and private, redacted and un-redacted faces of Diebold, this document is exceedingly relevant as we go into the November 7 elections. 468 federal seats and countless state and local contests are being decided by Diebold and other similar electronic voting machines. The outcome of these elections will set the direction of our country for the next two years.

The issue is whether Diebold has implemented the critical changes in its software and hardware called for by the full, genuine un-redacted SAIC Report. What makes this so very important is that the software, including the core “source code” that runs the machines that process and count almost all of America’s vote on November 7 is as secret as the formula for Coca Cola and recipe for Kentucky Fried Chicken. Why tabulators, for example, which act as nothing more than an elaborate abacus, have “proprietary software”, hidden from election officials, Secretaries of State, Attorneys General and even the Governor of every state, is a true mystery and raises huge and angry suspicions within the computer scientist and cyber security communities.

And no one, except these four private, for profit corporations, Diebold, ES&S, Sequoia and Hart, is allowed to see or inspect the software (and the core source code) to EVER know if the machines have operated properly or if there was, or is, malicious software that could alter the vote.

Now we come back to Linda Lamone.

It seems that Maryland’s Board of Elections, under orders from Maryland Gov. Robert Ehrlich, hired another firm, Freeman, Craft and McGregor, to review the vulnerabilities identified in the SAIC Report, the real one, and confirm to the Governor and the State that they had all been fixed.

The Freeman report has been completed but Linda Lamone, despite briefing her own staff about it on August 11, 2006, refuses to disclose its contents to Governor Ehrlich and even refused to release it to her board, saying it was "proprietary" until this past Monday. Some officials in the Maryland government question whether Lamone's loyalties are with Diebold or the voters of the sate.

But, Lamone's dictatorial control over information in Maryland doesn't stop there.

Remarkably, Lamone didn't even allow Giles Berger, the Chairman of the Board of Elections, to see the original, un-redacted SAIC report. He and his staff – the people who were charged with oversight over the execution of elections and the training the local boards on these machines – have only been allowed to see the much smaller report, redacted and altered by Diebold.

What is she hiding from the State of Maryland? What is she, and Diebold, hiding from America's voters??

As a result of the courage of a top Maryland official, the entire SAIC report, showing the Diebold edits, omissions and additions, was just made available.

Now we can see, precisely, what Diebold is . . . and should be, afraid of!

The full State of Maryland Electronic Voting System Security Study, conducted by the SAIC and delivered to Maryland on September 17, 2003 is 152 pages plus 41 pages of appendices. The report that Linda Lamone handed to the Governor and to her own Board members was only 38 pages. 38 pages!

In total there are hundreds of edits, omission and additions. Here are a few examples:

Table of Contents page VII

Original SAIC Report:

Chapter 5: Risk Assessment Results, Steps 2 – 9

5.1 Step 2: Threat Identification

5.2 Step 3: Vulnerability Identification

5.3 Step 4: Control Analysis

5.3.1 Management Controls Analysis

5.3.2 Operational Controls Analysis

5.3.3 Technical Controls Analysis

5.4 Step 5: Likelihood Definition

5.4.1 Likelihood Rating Rationale

5.5 Step 6: Impact Analysis

5.5.1 Impact Rating Rationale

5.6 Step 7: Risk Determination

5.7 Detailed Risk Assessment Results

Submitted Report: Risk Assessment Results Chapter Completely Omitted

Executive Summary Page 2

Original SAIC Report: In response both SBE (Maryland State Board of Elections) and Diebold stated that the devices do not operate on the Internet, and that the State's procedural controls reduce or eliminate many of the vulnerabilities identified in the report.

Un-submitted Edited Version: In response both SBE and Diebold *affirmed* that the devices do not operate on the Internet, and the State's procedural controls reduce or eliminate many, *if not all*, of the vulnerabilities identified in the report.

Submitted Report: Completely Omitted

Executive Summary Page 3

Original SAIC Report: Risks identified were predominantly associated with a wide variety of administrative controls for voting system security. Among management and operational controls, SAIC found risks in the controls on access to servers, administration of passwords, use of system audit logs, intrusion detection and level of security training for elections personnel.

SAIC concluded that with the management and operational procedures currently in use, the risk of system compromise is high. SAIC indicated however that these vulnerabilities can be mitigated by adequate security planning and administration

Edited Version: Risks identified were predominantly associated with a wide variety of ABSENT administrative controls for voting system security. Among management and operational controls, SAIC found risks in the controls on access to servers, administration of passwords, use of system audit logs, intrusion detection and level of security training for elections personnel.

SAIC concluded that with the management and operational procedures currently in use, the risk of system compromise is high. SAIC indicated however that these vulnerabilities can be mitigated, *if not eliminated,* by adequate security planning and administration.

Submitted Report: Completely Omitted

Page 5

Original SAIC Report:

2.1.4 SBE does not require the secure transmission of election vote totals

"The SBE does not require encryption for the election results transmitted from the local polling sites to the LBE. Those results are transmitted over a private, point to point connection, via modem. Those transmitted results become the official results after the

canvassing process is completed. A 100% verification of the transmitted totals to the original PCMCIA cards (i.e., computer memory storage of actual vote totals) or the paper totals is not performed."

Submitted Report: "The SBE does not require encryption for the election results transmitted from the local polling sites to the LBE. Those transmitted results become the official results after the canvassing process is completed. A 100% verification of the transmitted totals to the original PCMCIA cards (i.e., computer memory storage of actual vote totals) or the paper totals is not performed."

Page 6

Original SAIC Report:

8. Controls are not implemented to detect unauthorized transaction

attempts by authorized and/or unauthorized users

There is no documentation that describes security controls for detecting unauthorized transaction attempts by authorized or unauthorized users. Therefore, the application of security controls may be applied inconsistently, incorrectly or incompletely.

Since a threat source is more likely to exploit a system if the evidence of his/her actions cannot be gathered or will go undetected, failure to have controls for detection increases the likelihood of system attacks, and consequently, of system compromise:

Submitted Report: Completely Omitted

Page 7

Original SAIC Report:

2.1.9: No documentation currently exists regarding appropriate access controls to the AccuVote-TS voting system

There is no documentation that identifies the process for maintaining appropriate access controls to the AccuVote-TS voting system. Without proper documentation, the consistent implementation of security controls cannot be verified or validated.

The lack of proper documentation has resulted in the vendor default settings being left in place with the default user ID in the configuration. This information (i.e., passwords) is also documented in various manuals.

Failure to correctly document access procedures, and use of vendor default passwords allows anyone with access to those documented passwords authenticated user privileges to the system. That access would allow the unauthorized user to do anything the legitimate user could do.

Submitted Report: Completely Omitted

Page 8

2.3.1 Audit logs are not configured properly and are not reviewed

Original SAIC Report: The GEMS server audit logs are not configured to log any security events (i.e., extended logging) at the operating system level and the current log size is too small. Consequently, recorded events are overwritten. In addition, the audit logs are not reviewed.

Failure to properly log and to review those logs makes it significantly more likely that an intruder's actions will not be detected. Assurance on non-detection may encourage a possible intruder to attempt a penetration of the system.

We recommend that the Windows 2000 operating system be configured to audit all security events and the log size should be set to an appropriate size. We also recommend that the event logs be reviewed on a regular basis.

Submitted Report: Completely Omitted

Despite its original date, and certain Diebold claims that all problems have been remedied with its machines, the report is considered to be a serious "smoking gun" by all computer experts who have seen it. It is evidence, they say, of a very purposeful plan by Diebold to hide the operational and security flaws on the machines that count all of the votes in Maryland and Georgia and many of the votes in states across the country.

The extreme sensitivity to investigation of Diebold voting hardware and software by Linda Lamone, the person who many say is responsible for selling Diebold systems to election directors across the country and even internationally, played out in a highly unusual unaired network television interview. Lamone, the former President of the NASED, was chiefly responsible for making recommendations to other states on which electronic voting machines they should use. Lamone is acutely aware of the problems associated with Diebold voting machines, yet remains steadfast in her defense of them. In her offices in Annapolis, Maryland last month, with a Diebold touch screen voting machine proudly displayed right behind her, Lamone abruptly stopped our interview, ripped off her microphone and walked off when I asked about the source code – and whether she believed its counting software should remain secretly controlled by Diebold.

Abrahams: Alright so you don't want to talk about the source code issues at all? (Lamone shakes head no) It is not relevant that we know that source code has been viewed?

Lamone: (looking at someone off camera) Yeah the ITA did it. And that whole system has been taken over by the national Institute for Standards and Technology in partnership with the election assistance commission. We are because I am participating in this are writing new, we have written new standards against which the voting systems are going to start being tested next year. I am participating in another project with the election assistance commission to write management guidelines covering security and other issues for election officials across the United States.

Abrahams: The reasons honestly why I ask the questions about the source code is because there are a lot of people out there- elected officials and scientists who say even if the machines are secure when those memory cards are taken to the tabulator and those tabulators count the votes we don't know how the votes are counted. The state doesn't know and the state has not been able to see the source code so it is an issue of voter confidence.

Lamone: I think you are in fantasy land. (speaking to someone off camera) I think I want to end this.

Abrahams: I am not in fantasy land- I just have a couple more questions

Lamone: No (takes off her microphone)

Abrahams: You don't want to finish? I just have a couple more questions…

Lamone-: No! (Finishes taking the microphone off and speaks to someone off camera)

Abrahams: I don't know why you don't wish to continue this. I am asking you legitimate questions relating to the Diebold voting systems.

(Camera holds on empty chair with the Diebold Electronic Voting Machine, sitting alone, in the immediate background)

Given the voting breakdowns in Maryland during the September Primaries and the upcoming November 7 Midterms, the edits to the SAIC study and the reactions of Lamone during the interview are of great concern to those studying electronic voting.

This is ever more so, according to the experts, because in 2002, under the Help America Vote Act (HAVA), America totally turned its elections, and in a very real sense, its Democracy over to Diebold and three other private for profit corporations – ES&S (Election Software & Systems), Sequoia and Hart Intercivic.

These four corporations make the E-poll books that now hold America's voter rolls, the electronic voting machines that process America's votes and the tabulators that count America's vote.

There is still time, for a courageous Secretary of State, Attorney General or Governor, to stand up and publicly demand that Diebold and the other manufacturers do the following:

1. Prove that the many recommendations, contained in the un-redacted SAIC Report, have been complied with.
2. In Maryland, release the Freeman, Craft, McGregor Report showing what, if anything has been fixed since the SAIC Report
3. Make the electronic voting machines and tabulators available immediately before, during and after the November 7 election for identified, certified computer scientists from the state government, (an "Election Swat Team") to inspect for evidence of tampering, factory installed malicious code, malicious code that might have been added after leaving the factory, malicious code that might have been added during the election.
4. Make emergency Paper Ballots available for all voters who are not comfortable trusting the electronic machines. If the counties across this country have to pay Rush Fees to printers in their jurisdiction, so be it. Democracy demands nothing less.

We do not have only Diebold to blame for the critical position the un-redacted SAIC Report shows we are in. The Federal Government, despite mandating these machines has refused to exercise any oversight over them and bears huge responsibility, from The White House to the Congress.

George Bush's own appointee to the Chair the EAC, The Election Administration

Commission, Rev. DeForest Soares, quit that post, stating, rather dramatically that, “There is no prototype. There are no standards. There is no scientific research that would guarantee any election district that there’s a machine that can be used to answer these very serious questions. And so, my sense is that the politicians in Washington have concluded that the system can’t be all that bad because, after all, it produced them. And as long as an elected official is an elected official, then whatever machine was used, whatever device was used to elect him or her, seems to be adequate. But there’s an erosion of voting rights implicit in our inability to trust the technology that we use and if we were another country being analyzed by America, we would conclude that this country is ripe for stealing elections and for fraud.”

And Congress has refused to do anything to protect the voters or the Democratic process.

Congress refused to require that the four manufacturers make the software available for inspection (the Independent Testing Laboratories only perform tests on the machine’s functionality.) They do not even look (and they’re not required to look) for vote-flipping malicious code inside the software. Congress refused to require voter verified paper trails where the voter would look at a paper receipt inside the machine (not take it home with them), verify that it was correct and then allow for it, the hard copy, to be stored separately. And, further, Congress has refused to require mandatory random audits at polling stations or any other verification that the totals that are reported are, in fact, anything close to what they should be.

And, it is unlikely that Congress will ever solve the problems indicated in the SAIC Report. Republican Senator Mitch McConnell, the man who will likely become Senate Majority Leader, (together with convicted Ohio Republican Congressman Bob Ney) lead the effort to keep legislation requiring voter verified paper trails and machine transparency from ever coming to a vote in Congress, and even urged their Congressional colleagues to vote against any efforts to do so (see “Dear Colleague” Letter on March 3, 2004)

See contents of that letter here.

See ABCNews.com blog here: Political Punch

In other words, despite the brilliant rallying cry of their hero, Ronald Reagan, “Trust but Verify”, the Republican Leadership has, in fact, created a Democracy where we are asked to do one but with no effort at all to do the other.

The leaked, un-redacted SAIC Report makes it clear that these machines are not ready for our midterm elections next week and that Diebold, and, perhaps the three other manufacturers, have been fraudulently hiding serious operational and security flaws from the states and the voters.

Unless there is emergency action undertaken by our states, we could have 468 mini Florida 2000s and the control and direction of our Congress debated for many months to come. Nonetheless, absent the ability to properly inspect the software on these machines, the best safeguard may, indeed, be for everyone to vote. The larger the turnout and, conceivably, the larger the margin of victory, one way or another, the less likely these far from proven machines will be able to alter the vote in defiance of the exit polling.

Until we can get Diebold and the other manufacturers who hold our democracy in their corporate hand to tell the truth about their hardware and software, our democracy may

hinge on people doing what it is really all about anyway, getting out and voting.

Articles by: **Rebecca Abrahams**