# Independent Verification: Essential Action

# to Assure Integrity in the Voting Process

by

**Roy G. Saltman**
**Consultant and Author on Voting Technology**
**rsaltman@alum.mit.edu**

submitted to

**National Institute of Standards and Technology**
**Gaithersburg, MD 20899**

under

**Order No. SB134106W0703**

**August 22, 2006**

## ABSTRACT

Audit trails are needed for direct-recording electronic (DRE) voting systems. The widely used, current method of providing an audit trail with printouts is evaluated, and several disadvantages are noted. Advocates for blind persons claim that use of the printouts is discriminatory and unlawful. Software fraud or error is a major concern of computer scientists. The issue arose in 1969, soon after use of computers in voting began. Document control and partial recounting were recommended solutions for systems using ballots, but controversy remains over DRE systems, even though non-ballot lever machines were successfully used for over 100 years. Some available independent verification devices (IVDs) are described. Recommendations are that independent verification would reduce the fear of fraud, a continuing concern over the more than 200 years of US elections, as well as improve integrity and public confidence in correctness of reported outcomes. Proposed performance criteria for IVDs are given. An IVD should be connected to each DRE in use. Voting systems using hard-copy ballots should be required to undertake audits with independent recounts of at least 3% at no cost to candidates.


## TABLE OF CONTENTS

## 1. A History of Election Frauds and their Implication for Today

A significant fraction of the work of administration of voting in the United States concerns efforts to ensure integrity of the process. Frauds have been perpetrated in both urban and rural areas, and the reason for them is clear. In this country, the winning of elections is an important road to political power. Over time, political bosses in metropolitan areas as well as in rural counties have been denounced as maintaining power through election manipulation.

A recent book by this author on the history of voting technology (Saltman, 2006) references many previous texts that have detailed frauds undertaken from the time of the founding of this nation through the mid 20th century. The book details, in addition, one allegedly fraudulent action concerning voter registration perpetrated before the 2004 general election; that situation has now generated at least one state law in response. There is no hard evidence that vote-counting fraud occurred in the 2004 election, regardless of conspiracy theorists claiming the opposite, but a few cases concerned with voter registration frauds and voter intimidation or bribery have been successfully prosecuted in the recent past.

A book published a year ago (Campbell, 2005) has the sole purpose of specifically detailing election frauds throughout US history. In a third book, a chapter entitled "Election Fraud: An American Vice" is included among others covering various aspects of US elections (Goldberg, 1987). The latter text reports one of the very few frauds known to have been carried out in a computerized voting situation. In 1985, in one precinct in Chicago, precinct workers ran a ballot card voted for their favored party through a precinct-located voting unit 198 times and another ballot card voted for the opposite party through the unit six times "for the sake of credibility." The extra ballots were covered for accounting purposes by the use of the names of voters who had not shown up to vote (Goldberg, 1987, p. 187-188). One-party dominance that is sufficiently severe to prevent a genuine bi-partisan presence at polling stations promotes the possibility of this type of vote fraud. Such a situation may occur in both urban and rural areas, with different parties dominant in the various regions.

Several types of election frauds may be distinguished:

(1) efforts to manipulate the number of persons voting, for example, by arranging for non-eligible persons to vote, by intimidating persons who could lawfully vote into not voting, or by deliberately providing incorrect information to lawful voters to induce them to appear at the wrong polling place or at the correct polling place on the wrong day;

(2) efforts by private groups to accept voter registration applications from all persons and then submit to official registrars only those that mirror the group's own political bias;

(3) efforts to bribe or intimidate persons entitled to vote so that they will vote a certain way; and

(4) efforts to manipulate the vote-count to cause wrong totals to be announced and certified, which may occur in connection with fraudulent use of voter sign-in records on election day.

This report concerns the assurance of integrity in vote-counting, and therefore is relevant only to fraud type (4).

There may or may not be attempts at vote-counting frauds today but, certainly, the history of frauds remains lodged in the public's consciousness and engenders suspicion as an *a priori* condition. Furthermore, the publicity given conspiracy theories now circulating raises more doubts. This situation requires implementation of additional measures to assure public confidence.

## 2. The Effects of Different Voting Procedures and Technologies

At the time of the founding of this nation, some voting was done with paper ballots and some was accomplished orally. Ballots are a type of artifact. In ancient times, artifacts used for voting might have been pebbles, beans, small balls, or pieces of pottery or natural shell. (The word "ballot" comes from the Italian for "small ball.") In the area that became the New England states, paper ballots were generally used from the very beginning of voting. In Virginia, voting was done orally before a clerk who would ask the voter his choices and write down the responses. Thus, originally, the US had both artifact and non-artifact voting systems.

Obviously, oral voting was not secret, but a positive attribute was that the results were indisputable. By the time of the Civil War, most states that had previously employed that technique had converted to voting by ballot. Often, a stated reason for elimination of oral voting was intimidation by creditors, landlords, and employers threatening respectively their debtors, tenants and employees. A second reason for the change was that counting ballots was a less time-consuming process when the turnout was large. A few states were holdouts, and in 1871, the federal government adopted a law requiring voting by ballot for members of the House of Representatives. The Congress has authority under the Constitution to dictate the "manner" of voting for federal elections but not for state elections. Nevertheless, the law made no mention of voting for Presidential Electors; US Senators were still being named by state legislatures at the time. The last state holding out against voting by ballot was Kentucky, which did not fully adopt it until 1891.

In the 19th century, up to its last decade, most ballot voting was not secret, even though secrecy was often a stated reason for replacement of oral voting. Ballots were printed and distributed by the political parties, and were of different sizes and colors. (A state law requiring that ballots be "white" was easily circumvented because different shades of white could be used.) Observers at polling stations could identify which party's ballot a voter inserted into a ballot box. Voters could vote a split ticket; small pieces of paper with candidate names on them (called "pasters"), as well as paste pots, were sometimes made available at polling stations. The pasters could be glued over printed names on the ballot. Thus, the activity of casting a split ticket took extra effort.

A reaction against paper-ballot frauds became stronger as the 19th century progressed. Systems

of records of registered voters were primitive or non-existent at the time. That situation facilitated the fraud of stuffing extra ballots into ballot boxes and the use of paid "floaters" who were given other persons' names and addresses to vote at many polling stations. Other types of frauds included distributing counterfeit party ballots which actually listed opposition candidates for one or more offices, stealing and destroying ballots already cast and replacing them with pre-marked ballots, bribing counting clerks to surreptitiously mark ballots with extra strokes that would classify the ballots as unlawfully indicating that bribed voters had carried out their bargains, and bribing counting clerks to misreport totals.

A second reaction was against non-secret voting. As the economy became industrialized, there began to be masses of workers who were intimidated by their employers. A significant interest group thus was formed. The result of the desire for greater integrity and secrecy was the implementation of two new voting methods.

One new voting method was the replacement of separate party-issued ballots by a single neutral ballot containing the names of candidates of all parties for all offices. This "Australian" ballot (named for the nation where the concept first originated) was issued only by official election authorities and was made available only at polling stations on election day. This procedure prevented the issuance of counterfeit ballots and eliminated the turmoil and violence which had occurred outside of polling stations as party activists attempted to force voters to accept their particular ballot. Voters' choices were now secret, as the same form of ballot was used by each voter, regardless of the varying selections. An example of this type of ballot is shown by Saltman, 2006, p. 101. The first state adopting the Australian ballot statewide was Massachusetts in 1888, and by 1896, about 40 states, one-by-one, began to use the process. There was never a federal law or requirement; adoption and implementation was by the states themselves.

The second new method was the invention and deployment of the mechanical lever voting machine. The seminal invention occurred in 1889 and the first use in a federal election was in Rochester, New York, in 1896. The advantage of the machine was that it did not employ paper ballots and therefore no paper-ballot frauds could be perpetrated. (It has its own serious internal design defect, described below, which never generated demands for "paper trails" or the machine's abandonment.) Furthermore, since voters did not fill out ballots, they could not make non-standard marks; unapproved marks had raised the issue of "intent of the voter" and there were heated debates and lawsuits as a result of close elections concerning the intent of voters who had cast the crucial ballots. Thus, the type of dispute that occurred in Florida in 2000 has a long history.

The voting process with lever machines was secret, also. In the initial implementation, the voter entered a private, enclosed area (a "booth") where voting was carried out but, in later designs, the voter was protected from being observed by a curtain. The machine's face had the appearance of an Australian ballot, with each party's candidates in a separate parallel column and the various offices presented in separate parallel rows. In the initial design, a voter selected

a candidate by pushing a locking push-key next to the candidate's name and later, using a subsequent invention, by positioning a small lever pointing to the candidate's name. The use of the lever made it possible for the voter to change a selection, not possible with the locking push-key. The sum of the votes for each candidate was indicated on a separate counter hidden inside each machine. The values could be viewed after voting ended and the machines were opened.

Diffusion of this type of machine slowly occurred and, by 1964, almost two-thirds of all US voters were using it. In that year, almost all other voters were using paper ballots that were hand-counted, and the remaining few were employing newly deployed computer-readable paper ballots whose holes or marks, indicating votes, were automatically sensed. In the late1970s and early 1980s, mechanical lever machines began to be replaced in small percentages by their computer-based direct-recording electronic (DRE) equivalents, and that conversion has continued through the present. Some of the mechanical devices continued to be used in 2005 state elections, for example, throughout New York. (In 2006, the US Department of Justice filed a suit against that state. New York had accepted funds under the federal Help America Vote Act of 2002 but had failed to utilize the funds for agreed purposes, such as the replacement of its lever machines or development of a statewide computerized voter-registration file.)

Thus, at present, US voters may find artifact-based or non-artifact voting devices at their polling stations. Non-artifact voting, first orally, then with mechanical lever machines, and more recently with DRE machines, has been used somewhere in the US since the first votes were taken in the original states. Non-artifact voting systems require special techniques for design and implementation to enable independent verification to be carried out.

## 3. Concern over Software Fraud Begins

Soon after computerized voting with punched cards began to be used in 1968 in Los Angeles County, the question of the possibility of fraudulent software arose in that region. The issue was highlighted in a page-one story in *The Los Angeles Times* (Bergholz, 1969). The article described an experiment undertaken by a group of computer scientists. The group was divided into two. One sub-group secretly changed a computer program that was to count votes on ballots by adding a bias routine, and the second group was supposed to find the added code. In the experiment, the attacking sub-group seemed to have the edge; the defenders could not find the malicious routine because it had erased itself after performing its nefarious work. This fact highlighted the insidious nature of program manipulation.

The newspaper story created a stir in the Los Angeles area. The county government established an Election Security Committee to review the situation. Later, that government, as well as the California State Commission on Voting Machines and Vote-Tabulating Devices, let a number of contracts to specialists who further analyzed the issues. Additionally, articles by technical experts proposing remedies were written in journals for computer professionals. Recommendations from all of these efforts, identifying methods of preventing software fraud, were reported and categorized into differing subjects as follows (Saltman, 1975, pp. 35-38):

(1) require audit trails of computations;
(2) limit physical access to systems;
(3) allow observer teams to watch proceedings;
(4) undertake recounting;
(5) set requirements for design of computer programs;
(6) carry out testing of computer programs;
(7) improve security of computer systems and operator procedures;
(8) review and achieve better administrative management; and
(9) adopt and implement state-level regulations.

In 1969, when the concerns first arose, there were no national standards and no institutionalization of testing of computer programs used for vote-counting. A better institutional environment, suggested by (9), would arise slowly. California has taken the lead among the states with the development of significant state regulatory activities. A role for the federal government, an issue not raised in the Los Angeles recommendations, eventually was considered by Congress. The Clearinghouse on Election Administration was established in 1972 and moved into the Federal Election Commission (FEC) in 1975. The development of the first federal voluntary standards began in 1984, and their completion and issuance occurred in 1990. The process of certification of independent testing laboratories (ITAs) was started soon afterwards. Finally, federal institutions specifically focused on the effective administration of elections were created in 2004 under the Help America Vote Act of 2002 (HAVA). ITAs are now called Voting System Testing Laboratories (VSTLs).

The items above that primarily demonstrate a concern for computer security are (2), (5), (6), and (7), while items (1) and (4) refer to assurance of accurate calculation and reporting of the election results. From the very first, the question of computer security would dominate application of resources to assure integrity, even though implementation of audits would reduce reliance on computer security to provide total assurance of accurate reporting of outcomes.

The distinction between assurance of accurate calculation and reporting of the election results and the assurance of computer security may be described with an analogy. Consider a vehicle carrying a load of goods from seller to buyer. The assurance of the vehicle's safe arrival at its destination is the result of adequate maintenance by its mechanics and safe navigation by its driver. Hiring criteria for these individuals should have included competence and honesty. However, the safe arrival of the vehicle is not the end of the transaction. The goods must be examined to assure that they are exactly those ordered and that they have arrived in good condition. The vehicle is analogous to the specialized computer on which the election application runs, and the assessment of the goods upon arrival is the equivalent of an audit of the election.

The demand since 2003 for "paper trails" for DREs does not fully reflect the total requirements for assurance of the accurate reporting of election outcomes for those machines. A paper trail is a printout from a DRE of the choices made by a voter, and is to be reviewed and approved by the

voter as the last step of the voting process. See Section 9 below for a more complete discussion of paper trails, including their disadvantages.

## 4. Inclusion of Electronic Audit Trails in Designs of DREs

In the design of mechanical lever machines, overvotes are prevented by mechanical interlocks, not possible with voter-filled-out ballots without the assistance of computerized ballot-sensing at polling stations. However, an important and negative feature of lever machines is that no audit trail is retained. An audit trail is defined here as the retained sets of votes cast by all voters. The identity of each voter is divorced from the set of votes cast because state laws generally require a secret ballot. In use of a lever machine, after the voter completes selections and opens the privacy curtain (which causes the levers to return to their neutral positions), no record of the voter's individual choices remains. The voter's selections are added to the values in respective arithmetic counters storing the total count for each candidate, and only each candidate's running sum of votes is stored. HAVA requires, in section 301(a)(2)(A), that "In general – the voting system shall produce a record with an audit capacity for such system." This statement appears to imply that that mechanical lever machines are no longer lawful for use in federal elections.

DRE machines were originally designed to simply replace the mechanical operation of lever machines with electrical and/or electronically operating components, thereby continuing the prevention of overvotes and any question of "intent of the voter." However, by the time DREs were being developed, magnetic digital storage was possible. An improvement to the new type of machine was proposed:

> "Some assurance of the machine's correct operation ... may be achieved by the retention, in a more permanent form, of the set of each individual voter's choices that are determined by the machine. These voter-choice sets have to be retained in randomized locations so that no set of choices can be traced to a particular voter. ... The sets of voter choices on a particular DRE machine may be summarized on an independent DRE machine or general-purpose computer for verification.
>
> "With DRE machines, no independently created ballots are available for verification of correctness of <u>both</u> ... precise recording of the expression of each voter's choices, and accurate summation of all voters' choices to yield final results. Stored voter-choice sets may be used to verify only the <u>latter</u> of these two steps. The machine-produced recording of the expression of each voter's choices is not independent of the machine process that produced it. ***The machine cannot be used to independently verify its own correctness***" (Saltman, 1988, pp. 41-42). [Emphasis in the last sentence added here.]

The requirement for inclusion of voter-choice sets in DRE design was contained in the first set of national voluntary standards produced by the FEC in 1990. In that document, they are called "electronic ballot images (EBIs)." Apparently, the inclusion of EBIs with DREs is acceptable

under HAVA to meet the requirements for an audit trail. The printout of the EBIs following the close of polls and the ability of their records on magnetic disk to be recounted on another computer system appears to satisfy the needs of current law. However, many individuals who work with computers professionally are not satisfied with the law as currently interpreted.

## 5. Concern Rises over Use of DREs without Paper Trails

Despite their increasing deployment in US elections in the last quarter of the 20th century, there was no significant opposition to the use of DREs until 2003. In 2000, this type of voting device was used by about 13% of US voters, although none were used in the Florida presidential election of that year. By the 2002 federal election, their use had increased to 22% of the electorate (Brace, 2004). The growth was due, in large measure, to the recognition that the "intent of the voter" problem that had been clearly demonstrated in the Florida fiasco could be prevented with use of a voting device that did not employ ballots.

One may speculate as to why extensive opposition arose only in 2003. One possible answer is that many of the first DREs were operated by push-buttons or micro-switches and showed the entire ballot on the machine's surface. These had a similar appearance to their lever-machine predecessors. Lever machines had been used for many years without paper trails, as pointed out above and, while their deployment had decreased, they were still used by 15% of voters in 2002.

In the middle 1990s, a type of DRE using touch-screens was developed. With the use of this kind of DRE, the ballot was not made visible all at once, but had to be seen on a succession of screens. One possible source of concern may result from a drift in the voltage that reports to the computer program where a finger is touching the screen. On rare occasions, a slight change in voltage may cause a touch to be recorded as selection of a different candidate than desired by the voter. While the voter can see this error and easily correct it, it may be disconcerting and generate suspicion of malicious intent. Additionally, these machines have an appearance more similar to personal computers than other types of DREs, and most personal computers are often connected to the Internet. Around 2000, there were experiments of voting over the Internet. Examples of this were the Arizona Democratic and Alaska Republican primaries of that year. Widely publicized Internet hacking incidents that affected computer systems of large private businesses and government agencies raised fears that touch-screen DREs could be similarly impacted. (No connection of a DRE to the Internet is known to this author, but that reality may not be understood by much of the concerned public.)

It appears that many members of the public want something, if not a ballot, that they can touch in order to obtain proof that their votes have been cast exactly as intended. Persons who use ATM machines and those who buy gas at pumps by inserting a credit card in a slot can get a receipt. Voters seem to be asking: why can't we get something similar?

In October, 2002, use of DREs got a boost with the passage of HAVA. In Section 301(a)(3), the law states:

> The voting system [used in an election for federal office] shall--
> (A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that promotes the same opportunity for access and participation (including privacy and independence) as for other voters.
>
> (B) satisfy the requirements of subparagraph (A) through the use of at least one ***direct recording electronic voting system*** or other voting system equipped for individuals with disabilities at each polling place, … [emphasis added here]

This provision clearly promotes the adoption of DREs. Many jurisdictions not using them in 2002 contemplated their purchase. HAVA authorized distribution of three billion dollars to the states, provided that the states submitted plans specifying use of the money consistent with identified HAVA requirements. An acceptable use was the replacement of punched card or mechanical lever voting machines with either optical-scan or DRE systems.

Following are some examples of concerns about integrity of DREs, beginning in 2003.

In early 2003, David L. Dill, professor of computer science at Stanford University, actively opposed, with public testimony, his local county's contemplated purchase of DREs. He began the Verified Voting Foundation and established a website at www.verifiedvoting.org. He posted on his website a resolution which was afterwards endorsed by many information systems professionals. The resolution includes the following:

> "Computerized voting equipment is inherently subject to programming error, equipment malfunction and malicious tampering. It is therefore crucial that voting equipment provide a voter-verifiable audit trail, by which we mean a permanent record of each vote that can be checked for accuracy by the voter before the vote is submitted, and is difficult or impossible to alter after it has been checked ..."

In the summer of 2003, an experiment undertaken by Dr. Avi Rubin, a computer scientist at Johns Hopkins University, was widely reported by the media. Rubin and associates asserted, among other claims, that the "smartcard" given to each voter at polling stations in Maryland to be entered into a DRE machine in preparation for voting, could be easily duplicated; this would allow a voter to vote many times (Kohno et al., 2003). As a result, Maryland's government let two contracts to review security procedures, and some procedural changes were made. Rebuttal of the charges and corrections made were minimally publicized in the media.

In July, 2006, the possibility of "hacking" by just one person was highlighted in the presentation of a new report by the Brennan Center for Justice of New York University School of Law (Brennan Center, 2006). The limited conditions under which this "one person" might carry out the manipulation were not reported in the media. The report itself is considerably more detailed

and provides an excellent description of necessary responses to vulnerabilities.

On July 31, 2006, a press release from the Open Voting Foundation of Granite Bay, California, about a particular DRE machine, was headlined: "Worst Ever Security Flaw Found in Diebold TS Voting Machine." The text stated:

> "... it has been determined that with the flip of a single switch inside, the [Diebold TS] machine can behave in a completely different manner compared to the tested and certified version. ... According to [foundation president Alan] Dechert, 'If you have access to these machines and you want to rig an election, anything is possible ... and it could be done without leaving a trace. All you need is a screwdriver.' ..."

In December, 2005, the media reported an experiment by the Supervisor of Elections of Leon County, Florida. A computer security expert was permitted access to the internals of a computer used to count votes, and the expert altered the machine's program. Consequently, the machine reported an incorrect result in a mock election. The experiment was touted as another example of the vulnerability of vote-counting by computer, and it may be assumed that, as a result of the publicity, public confidence was further eroded.

What the media did not make clear in this case was that Leon County's voting system employs voter-filled-out optical-scan ballots. Thus, regardless of any malicious distortion of the computer program, the ballots themselves would be available to be recounted by hand or on an independently managed computer system to check the initially reported results. Limitations in computer security were highlighted but the available remedy of independent verification was ignored.

### 6. Testing and Assurance Activities of States Using DREs without Paper Trails

With opposition from professionals with the necessary technical credentials and the wide publicity given flaws in computer security, states using DREs at polling stations without paper trails have had to justify their procedures. Such states include Georgia, Louisiana, and Maryland.

**In Georgia**, Brit Williams, professor emeritus of computer sciences at Kennesaw State University (KSU) and technical expert for the state, has been actively defending his state's implementation. He spoke on the subject at a NIST technical symposium on December 10, 2003 and testified to the Committee on House Administration of the US House of Representatives on July 7, 2004, along with Kathy Rogers, Director of the Georgia Elections Division. He has noted that Georgia has created the Center for Elections Systems at KSU to provide support and independent testing for all of its 159 counties. Tens of thousands of voting system components are tested there and the staff continues to travel to each of Georgia's counties to independently test and validate all new equipment purchases. Georgia employs a method of testing its software

to assure that no Trojan Horse program can switch votes. After an election and the closing of polls, the results for each machine are posted on the wall of the precinct. Any manipulation of the memory cards during the time they are transported to the central processing station would be found out. A more complete review of Williams' presentations is available (Saltman, 2006, pp. 206-207).

**In Louisiana**, protective measures take advantage of the fact that this state formerly employed lever machines statewide and had developed procedures to assure their correct operation. A recent communication from the office of the Secretary of State provided the following information:

> "Every machine is tested prior to an election to assure it is working correctly and is voting correctly, i.e., it registers the vote to the correct candidate position and it produces a zero proof sheet. We have both a protective counter and public counter and each is checked on every machine before election. ... [The public counter] records the number of votes on that machine at that election. This can be checked with the precinct registers as our commissioners have voters sign the register before voting on the machine. ... A change in software cannot be made by [equipment vendor] Sequoia without our assistance/knowledge, nor could we make a change without Sequoia's assistance and knowledge. We have password-protected logons and we audit every logon and follow all activity in this regard. We also have limited access, of course, which depends on a person's level of authority in our department. ..."

**In Maryland**, the state assures the receipt of correct software from the vendor by obtaining it directly from the certified VSTL and not from the vendor. Furthermore, the software has an attached digital signature; a code appended to the program which is unique to the particular sequence of the program's data. The same software is also sent by the vendor to NIST's National Program Reference Library with a digital signature. The two digital signatures are compared and they will not match if the two programs differ in the slightest degree (with an extremely high level of probability).

Additionally, the Maryland State Board of Elections has made available a document describing various aspects of the voting system used in the state at:
www.elections.state.md.us/citizens/voting_systems/index.html

A description of some of Maryland's testing activities is as follows:

In Acceptance Testing, the first part of the test is a diagnostic to ensure that each voting unit and all of its components are performing to the required specifications; the second part of the test includes casting hundreds of votes on each voting unit.

In Logic and Accuracy Testing, hundreds of test votes are cast on each voting unit prior to an

election. For each touch-screen unit, more test votes are cast than there are registered voters in the precinct to which the machine will be assigned.

In Parallel Testing, two individuals read aloud the votes cast on a paper ballot and two people cast those votes on a touch-screen voting unit. After all votes have been cast, the hand-tallies are compared to the results generated by the voting unit, and the total should match. Parallel testing is conducted two times for each election. Parallel testing is first conducted in each county during the pre-election public demonstration and also on Election Day. In 2004, fifty ballots were cast and counted during the pre-election parallel testing. On Election Day, over 1,300 votes were cast.

In Post-Election Audit and Verification, local boards of election verify totals obtained by summation of each machine's results. They also conduct an audit to confirm the accuracy of polling place forms completed by election judges.

**Strong support for use of DREs without paper trails** has been provided by the testimony of Conny B. McCormack, elections administrator of Los Angeles County, the nation's largest local election jurisdiction. Ms. McCormack, in a presentation before the US Senate Committee on Rules and Administration on June 21, 2005, stated:

> "The fact is that existing DRE systems without VVPAT [voter-verified paper audit trails] have the proven track record of doing the best job of all available voting systems. ... The suppositions and theories espoused by critics contending that DRE systems are more susceptible to tampering are completely false ..."

Unfortunately for Ms. McCormack, California has required the use of VVPAT, so that she cannot employ DREs as she would desire. A problem in Los Angeles is the requirement of the Voting Rights Act amendments of 1975, recently re-authorized, that ballots be made available in any language used by more than 5% of the residents of the jurisdiction (see Saltman, 2006, pp. 144-145). In Los Angeles County, six languages other than English must be accommodated. With the use of DREs without paper, the ballots could be presented in a purely electronic manner, obviating the need for extensive printing. The adoption of political requirements into law often fails to fully consider the implications for implementation.

## 7. The Concept of an Audit

An audit, to quote a dictionary definition, is "a formal or official examination and verification," or "a methodical examination and review." The concept comes from the financial world, where an audit of accounting methods and records is a usual procedure. Audits are typically carried out by "internal auditors," who work for an organization needing reviews. Internal auditors report to the highest levels of management, in order to be separated from those who actually prepare accounting records. Internal auditors are concerned with implementation of specific "internal controls" that assure that the necessary operations are being carried out, and that those

operations are being carried out in an effective manner with integrity. In effect, an audit is an independent verification; those who carry it out are not the same persons who initially accomplished the work.

In auditing, correctness of the application is primary, and the security of the computers on which the application is being run is only one aspect of the examination. Auditing was carried out before computers were invented, and the concept remains the same, even if some techniques are different, now that computers are being used.

The concept of auditing has been applied to the voting process but, in some ways, the problem is more challenging. In banking, each depositor has his or her own account; deposits and withdrawals may be reviewed to determine if the balance in an account is consistent with account inputs and outputs. Each depositor may assist auditors in the review of activity of a personal account. However, in voting, deposits are made in a candidate's account by anonymous voters. Secrecy of the vote requires that no association is able to be made between the vote deposited and the identity of the voter who deposited it. Thus, no individual candidate's account can be separately reviewed by itself, by comparing the number of voters voting with a single candidate's total. All that can be known, without reviewing the actual ballots cast is that, in a vote-for-one contest, the sum of the number of votes cast for all competing candidates plus the number of votes failed to be cast (undervotes), plus those cast incorrectly due to overvotes, must sum to the number of voters voting in the contest. This calculation is called a "reconciliation." An audit of results of voting involves, at minimum, the necessary reconciliations. A more complete audit also would include a partial or full recount, independently carried out.

## 8. 1975 Recommendations for Internal Control and Audit

In one of the very first studies of the integrity of computerized vote-counting, this researcher was requested to investigate "independent audits of election processes" and "methods currently being employed to detect and prevent computer vote fraud" (Saltman, 1975, p. 1). At the time, nearly all computerized voting used hard-copy ballots. Mechanical lever machines were not computerized, and DRE machines were being used only experimentally. There were no recommendations concerning assurance of DRE correctness in that report.

An important concern of the report was protections against ballot frauds. It was recommended that all of the official ballots printed and distributed must be accounted for, and there must be assurance against use of counterfeit ballots. At each precinct, the number of blank ballots received must equal the sum of ballots voted, unused, spoiled and otherwise employed (Saltman, 1975, pp. 41-45). This additional reconciliation is intended to prevent "ballot stuffing," i.e., the addition of extra voted ballots to a ballot box. Furthermore, if there are missing votes that do not complete the total, or if there are more votes cast than voters signed-in to vote, these inconsistencies can be investigated and resolved.

In order to accomplish this necessary task, the appropriate data must be collected at each

precinct. There is documented evidence that, in some locations, poll workers are not making the effort to record the needed information or that incorrect records are being maintained (see sources cited by Saltman, 2006, pp. 218, 219, "*Manual collection of auditing data at precincts needs to be improved*."). If these reconciliations are thoroughly and correctly made, and prevention of use of counterfeit ballots is assured, then only the fraud of "vote-switching" can be perpetrated. The employment of independent verification through a recount is intended to provide a high level of confidence that vote-switching has not occurred.

Taking into account the advice given in the several analyses that followed the 1969 Los Angeles County imbroglio, recommendations of the 1975 report concerned maintenance of control over the number and disposition of all ballots, application of the concept of "separation of duties," physical controls over the use and retention of removable storage media and computer components, and aids in the audit of vote-tallying calculations. With regard to the latter, it was recommended, in a summary, that there should be "reporting of all undervotes and overvotes, [and] ballot reconciliation and machine recounting on alternate, independently managed systems" (Saltman, 1975, p. 5). Reporting of all undervotes and overvotes was recommended to make reconciliations possible. Recounting on independently managed systems was proposed because hardware and software were not trusted.

In the body of the report, the question of recounting was discussed in detail. It was stated that:

> "The advantage of a hard-copy machine-readable ballot is that an independent verification of the count is possible. Ballots can be recounted on a different machine or they can be recounted by hand. Machine recounting permits a larger recount with considerably less effort.
>
> "If a backup machine is available, and that is recommended as a good management practice, the ballots may be recounted on that machine. Further confidence in the recount may be expected if the management of the backup machine is independent of the organization managing the primary machine. An independent organization could be considered to be one that reports to a different elected official and receives an independent budget." (Saltman, 1975, p. 45)

Now, more than thirty years later, the recommendations for auditing of vote processing for systems using hard-copy ballots will not be very different. While technology has changed, the basic concepts have not. An extension of the concept to voting systems using electronic ballots must be undertaken. In addition, the question of selection of the percentage recount must be discussed, and for that purpose, the 1975 report will be revisited again.

## 9. Evaluation of Paper-Trail Implementations

In preparation for the elections of 2004, the government of Nevada adopted a requirement that all of the state's DRE machines must provide paper trails. Many other states, including California,

have followed Nevada's lead. During the voting process, after a voter indicates to the machine that voting is complete, a paper summary of the voter's selections is printed. The voter is supposed to review the printout, which is available to be seen under a transparent cover on the voting console but cannot be touched. If the voter agrees that the printout mirrors the selections made, a final approval button is pushed and the printout is stored. If the voter finds that the printout does not show the choices that the voter believed that he or she selected, the voter may reject the printout and vote again. A rejected printout is retained but is identified.

The purpose of the review of the printout by the voter is to prevent the possibility that selections actually recorded in the computer as the voter's final choices are different than the selections shown to the voter on the final electronic screen. This possibility could be caused by malicious code undetected by all previous examinations of the computer program. In a primary election in September 2004 in Nevada, after the DREs had been outfitted for paper trails, reviewers were invited to watch the voting process. It was noted by two highly competent observers, Conny B. McCormack and Dr. Richard G. Smolka, editor of *Election Administration Reports*, that very few voters actually reviewed their printouts. Most of the voters simply pressed the necessary button for approval without actually examining the printout.

If a voter thoroughly reviews his or her printout, the printout may be treated as a document ballot, that is, a ballot that can serve as clear evidence of the voter's selections. However, if a voter fails to review his or her printout, that printout remains just a piece of paper produced by a computer program that is not trusted. Thus, the reviewed printouts constitute an audit carried out with a sample, but the percentage of the sample is not known. The actual percentage of voters reviewing their printouts in any particular election cannot be calculated without every voter being carefully watched. Furthermore, it is not known to what extent voters who review their printouts really review all contests including those at the middle and bottom of the ballot.

An important determination beforehand is the identification of which presentation, electronic screen or printout, is to be the official one for counting purposes. In the process described here, it makes sense to declare the printouts the documents of record, since they are permanently in paper and at least some of them will have been perused for accuracy by the voters. The electronic records (EBIs), which should contain the same data as the selections shown on the electronic screen if there has been no program manipulation, are easily summarized as they are stored on removable magnetic media and may be inserted in a general-purpose computer for that calculation. Thus, results quickly obtained are likely to be from records not fully trusted, with the paper printouts held in reserve in case of a dispute.

The printouts will serve a valuable purpose if malicious code is identified, so that the election can be suspended or cancelled for program review. For this to occur, a voter would have to demonstrate to a poll worker that the selections shown on the printout are different than the choices shown on the final electronic screen. That is, the final electronic screen would need to be available at the same time that the printout is being reviewed, in order to demonstrate a difference. A serious allegation that the computer program has been compromised cannot be

accepted from the printout alone. Additionally, it will be necessary for the poll worker to have been given explicit instructions as to what action to take in this situation.

Potential Losses of Privacy: A voter who discovers malicious code through a comparison of the printout and electronic screen has performed a valuable service, but it must be noted that such a voter must lose his or her privacy of voting in the course of the demonstration of the inconsistency. In general, state laws require a secret ballot, so this procedure for identifying a manipulated program may have to be reviewed for its conformance with current statutes. A second source of loss of privacy could occur due to the manner in which the printouts are retained. The printouts are typically stored on a roll, in the sequence in which they were voted. As a result, a review of the printouts without randomizing their sequence could identify the voters who generated them, if the sequence is compared to the sign-in list and the particular machine on which a voter voted is known.

Increasing Time to Vote: The addition of a paper trail to a DRE and the necessary comparison with the electronic screen to make the paper trail useful increases the time to vote. This fact was noted in a recent study of some vote verification technologies (Norris, Sears, and Nicholas, 2006). It was pointed out, also, by Conny B. McCormack in her testimony to the US Senate Committee on Rules and Administration. "Printing the paper record adds more time to the voting experience. Everyone is in agreement that it is anathema to voters to add waiting time," she stated.

Human Factor Concerns: Significant ergonomic issues have been raised with the use of paper trails with DRE machines. "The VVPT [voter-verified paper trail] is in a different format than the ballot ... and has a different graphical layout with different contrast and lighting parameters," according to an informal paper published in April 2004 as part of the Caltech/MIT Voting Technology Project (Selker and Goler, 2004). These differences would increase the difficulty of making a comparison, according to these researchers. "Comparing dozens of selections on a voter-verified paper receipt will take special care. Complications of comparing a separate paper trail in a different ballot format might add extra difficulty for people with learning or reading difficulties," they wrote. A study on usability of various vote-verification technologies stated that "questions were raised about the paper record's utility when used for a long ballot" (Center for American Politics and Citizenship, 2006).

Legal Issue of the Inability to Read Paper Trails by the Visually Handicapped: Section (301)(a)(3) of HAVA quoted above in Section 5 raises issues about the use of paper trails because visually impaired individuals cannot use them. Such voters cannot have, according to a particular interpretation, "the same opportunity for access and participation" in the use of paper trails as other voters. An article of August 2, 2006, posted on the Internet from the *Contra Costa Times* of Contra Costa County, California, states that three disability groups, including the American Association of People with Disabilities, have filed a lawsuit against the California Secretary of State and several counties in that state. The disability groups state that the defendants violated HAVA "by having its touch-screen voting machines produce a paper receipt

of votes, [and] that requirement denies blind voters the ability to verify their vote because they cannot read the receipt." The disability community has previously raised this concern about proposed laws mandating paper trails introduced for Congressional consideration. Thus, a lawsuit filed in a state that requires paper trails with DRE machines has been expected.

## 10. Some Currently Available Independent Verification Devices (IVDs)

This researcher does not have a financial interest in any voting device or system mentioned here, and does not claim to have reviewed all possible systems meeting the requirements for independent verification or those meeting HAVA requirements for equal participation by voters with physical handicaps.

Generation and Verification of an Optical-Scan Ballot with Audio Assist: This product is made by AutoMARK Technical Systems of Chicago and Lombard, Illinois, and marketed by Election Systems & Software of Omaha, Nebraska. The device provides a blind voter with an audio assist to navigate a touch-screen and select voting choices. (A sighted voter may use the system without the audio assist.) A vision-challenged voter can be assisted also to select a write-in candidate if that is desired. When the voter notifies the voting system that the selection process is complete, an optical-scan ballot is printed. The voter handles the ballot and manually transfers it to the entry slot of an optical-scan sensing unit for summation of the choices with the selections of other voters. The ballot, printed for easy recognition by an automatic sensing unit, may be visually scanned for correctness by a sighted voter, since the entries are human-readable (not encoded). The handling and entering of the ballot into the sensing unit by the sighted voter is sufficient evidence that the voter approves of the ballot as printed. A blind voter cannot read the ballot as he or she handles it, but that type of voter may use an audio assist in the sensing unit to verify that the selections on the ballot are exactly those chosen, making the ballot a voter-approved document for that type of voter. The system has the ability to allow voters with other types of disabilities to select voting choices with a puffing straw or with foot pedals. The system is now being used in Idaho, South Dakota, and Sacramento County, California, according to information on the company's website, www.automarkts.com.

An optical-scan ballot generated by this system is more than equivalent to such a ballot filled out by the voter using a manual method; it has some better features. The system-generated ballot is assured to contain no overvotes nor incorrect markings that would raise questions of "intent of the voter." As with optical-scan ballots filled out manually, these ballots may be recounted by hand or on an independently-managed computer system, and thus provide the basis for an audit, either partial or full.

Copying of the Voter's Final Choices by Capturing the Video Display Signal of a DRE: This device, called VoteGuard, is produced by Democracy Systems of Ormond Beach, Florida (www.democracysystems.com). According to literature from the company, the device receives the video from the "video out" connection of a DRE voting machine. Throughout election day, the VoteGuard device, positioned near the DRE, receives every screen displayed on the DRE as

well as all audio output from visually handicapped voters. The company states that "the recording process is an independent, passive recording of the DRE which means VoteGuard in no way communicates directly with the software running on the DRE unit itself." After the close of polls, the company's associated product, called VoteCube Analysis Server, which apparently has computational capability, is called into play. It is used to identify the specific data to be employed in the generation of a set of summary reports. Five types of reports may be produced. In the opinion of this researcher, the necessary requirement for independent verification is the capture of the voter's final set of selections and the independent summation of the choices on them for comparison with the DRE's results. The system does not generate individual ballots. As of the date of this report, the company's released information has not included a notice of any sales to election authorities.

Independent, Interactive, Computer-based Verification Module (VM): This product has been developed by Scytl of Barcelona, Spain. In operation, a copy of the voter's choices is received by the VM, a small box situated near the DRE. The face of the VM includes a screen and two pushbuttons to be used by the voter. The final set of votes cast by the voter is displayed on the VM's screen and/or is recited through headphones for a voter who is viewing or listening. The point within the DRE from which the data are taken and transferred to the VM is not specified in the descriptive literature from the manufacturer. The pushbuttons permit the voter either to "confirm" or "reject" the set of voter's choices displayed or spoken. Following the voter's confirmation, the record of the votes is encrypted and digitally signed. (If the votes are rejected, the voter must begin again to determine his or her selections.) The protected set of votes is stored in the VM and a positive verification message is sent back to the DRE. Following the close of polls, the encrypted votes are decrypted using keys previously assigned to various election authorities. The total of the votes for each candidate is calculated in the VM and compared in software with the corresponding totals from the DRE. The software of the VM is open to public review, according to a descriptive article by a technical expert available on the Scytl website, www.scytl.com.

Voter-Verified Audio Audit Transcript Trail (VVAATT): This system was developed by Professor Ted Selker of MIT, Cambridge, Massachusetts. The VVAATT is a voice-operated tape recorder that is connected to a DRE voting machine. While voting, the voter wears headphones. Each time that the voter makes a selection or de-selection on the DRE machine, the system determines the action taken, converts it to audio through voice synthesis, and sends that message to the headphones. The voter is able to verify that the actions that he or she has taken are being recorded correctly. (Norris et al, 2006, pp. 25-26, or search VVAATT on the Internet.)

After the polls are closed, election judges may review the audio tape, identify and sum votes cast for each candidate, and compare the results with those produced by the DRE voting machine.

End-to-End Voter Verification of Election Integrity: This system has been developed by VoteHere of Bellevue, Washington, now a division of Dategrity Corp. It requires a proprietary device called Sentinel associated with each DRE voting machine, as well as VoteHere

Management Tools, a computer program mounted on computers dedicated to election auditing at state and local government headquarters. The audit is set up from a central location before the election. The process requires authorities to perform a few tasks on a computer with help from the VoteHere Management Tools. At each polling station, Sentinel devices plug into each DRE, and the Sentinel receives the data about each voter's choices. Pictures of the Sentinel device do not show a screen. According to one description of this system (Norris, Sears, and Nicholas, 2006, pp. 29-34), "In the voting booth, the voter engages in a verification process, producing a receipt that the voter takes home." This verification process involves the use of mathematical cryptography, interaction among the Sentinel, DRE, and the voter, and the printing and displaying of sets of characters generated by the Sentinel. The printing is from the Sentinel and display is on the DRE's screen. The receipt obtained by the voter contains a set of characters that the voter may use on an Internet website after he or she returns home. The receipt is used to verify that the same set of characters is included on a list of identifiers of ballots on the website that have been accepted for tallying. Apparently, the receipt may be received in Braille for the benefit of visually handicapped voters, but this researcher has been told by a representative of the visually handicapped community that only a limited percent of blind persons can use Braille. After the close of polls, the election officials remove a memory stick from each Sentinel and return with it to the dedicated audit computer where the audit of the results is completed.

**11. <u>Comparison of Partial versus Complete Independent Verification</u>**:

In Section 3 above, the 1969 controversy over the possibility of software fraud was discussed; proposed countermeasures were identified. As a result of this dispute, the state of California decreed that 1% of computer-readable ballots, but in no case less than six precincts, were to be recounted by hand in all election contests. This rule is a requirement for partial independent verification, and it remains in effect at this time. DRE voting systems did not exist in the early 1970s when the rule was put in place.

<u>Voting Systems Using Computer-Readable Paper Ballots</u>: In the report of 1975, this researcher examined the question of whether a 1% manual recount was sufficient to identify malicious software that had the intention of switching votes to change the outcomes of elections (Saltman, 1975, pp. 113-121). It was pointed out that maintenance of control over the use of all ballots printed for the election was a necessary pre-condition for identifying any vote-switching that had been attempted. That requirement remains essential at this time. Vote-switching by a malicious program can be identified only if no other sources of change of results are possible due to mis-allocation of ballots.

The analysis of 1975 to determine a satisfactory percent recount proceeded with the assumption that a malevolent programmer could design a vote-switching scheme that would be difficult to detect by observation by knowledgeable reviewers of past election outcomes in the same jurisdictions. Comparisons of current election results with previous outcomes are often undertaken by political analysts to determine the changes in priorities indicated by changes in voting patterns by voters of the area. For example, knowledgeable observers have used recent

past history to counter unsubstantiated claims of fraud in the Ohio presidential election of 2004. A report of the Democratic National Committee, the party of the losing candidate, John Kerry, stated the following:

> "That the pattern of voting for Kerry is so similar to the pattern of voting for the Democratic candidate for governor in 2002 is, in the opinion of the team's political science experts, strong evidence against the claim that widespread fraud systematically mis-allocated votes from Kerry to Bush."

If the switching is limited to a very few precincts, and thus must be substantial in each of those precincts, then observers will recognize very unlikely outcomes. Thus, it was noted that:

> " ... an alert political party will keep good records of each precinct's voting patterns historically and with respect to similar precincts in the same election, thus minimizing the maximum level of undetectability by observation" (Saltman, 2006, p. 116).

However, clever schemes of vote-switching may attempt to reduce the number of votes switched in each precinct below the "maximum level of undetectability by observation," a parameter used in the 1975 analysis. The mathematical technique used in 1975 was independent sampling without replacement. The model assumed that every precinct contained the same number of voters and that each voter had voted for one of two candidates. The concept was that a malicious programmer had switched results in some precincts *but not others*, and the question was to determine the percent of precincts to recount such that at least one of the precincts whose votes had been altered would be recounted. The recounting would be expected to expose the fraud. If the switching was spread very thinly over all precincts in order to maximize the likelihood that it would not be noticed, a recount of almost any precinct would identify that a problem existed. It was assumed that, if more than a minimal difference was found between the original reported vote and the recounted vote in any precinct, the supposition would be that the computer program had been manipulated. Then, a decision could be made to examine the computer program, calling all results into question.

In the 1975 report, an example was given. In an election in which exactly one million votes were cast, in which the initial result given was 505,000 to 495,000, the difference between the candidates would be 1%, or 10,000 votes. To change the outcome, at least 5,000 votes would need to be switched. It was assumed that 1,000 votes were each cast in 1,000 precincts. Suppose the vote-switch has been achieved with a change of 50 votes each in just 100 precincts, and just 10 precincts (1% as in California) have been chosen to be recounted. Then, using independent sampling without replacement, the chance of selecting one of the 100 precincts whose results have been altered is 0.655. It was concluded in the 1975 report that a 1% recount was insufficient to provide a sufficiently high level of confidence that a manipulation, such as was postulated, would be found. In the specific example given, it would take a recount of 22 precincts (2.2%) to achieve a probability of 0.9 to choose for recounting one of the manipulated

precincts, a recount of 43 precincts (4.3%) to achieve a probability of 0.99 for selecting one of the manipulated precincts, and a recount of 64 precincts (6.4%) to achieve a probability of 0.999 of choosing one of the manipulated precincts. To achieve absolute certainty of discovering one of the bad precincts, the number of precincts to be recounted rises to 901 out of 1,000. Thus, there is a certain efficiency is not demanding perfection. (In the 2004 Ohio case, a 3% manual recount was undertaken, paid for by two minor parties also fielding presidential candidates. The recount resulted in minor changes in numerical results but verified the originally reported outcome.)

Tables are given in the 1975 report for levels of confidence of 0.9, 0.99 and 0.999 for finding at least one manipulated precinct for different numbers of precincts and different values of maximum level of undetectability by observation. As noted there,

> "as the candidate fractional difference ... gets smaller, the number of precincts to be recounted becomes larger and approaches the total number of precincts. This accords with what one would intuitively expect, and what actually occurs in practice. When there are very small reported differences between candidates, there is a high likelihood of a recount being demanded."

In 1975, a difference in a precinct's results between the original count and the recount of just one vote would not have been enough to call the entire election into question. The use of pre-scored punch cards, with their ambiguities of hanging chads, could easily cause the change in a few ballots without any indication of program manipulation. Similarly, with the use of optical-scan ballots, there is a likelihood that a manual recount could show a small change from the original count because of use of the wrong writing implement by the voter, or by the voter indicating a choice with a mark not readable by the computer's sensor, or by a degraded sensor that is not reading correctly. However, with optical-scan ballots, these types of problems are much more easily resolved than with pre-scored punch cards. The ballot is physically stable and careful handling (preventing smudges or bending) will not change the information on the ballot. A final determination of the choices on ambiguous ballots will help determine whether there was actual program manipulation in the precinct in question.

DRE Voting Systems: In this case, the equivalent question is the determination of which precincts should be instrumented with a product such as one of those described in Section 10. (The AutoMARK system may be eliminated from consideration here because it generates an optical-scan ballot, a highly unlikely choice in a situation where DREs are used at polling stations.) With DRE systems, there should be no difference whatsoever between the election results reported by the DRE machines and those generated by the corresponding IDV. There is no sensing of data on ballots and there is no opportunity for "intent of the voter" questions to arise. California officials manually sum the selections on all paper trails in 1% of precincts.

The answer to the question of percent instrumentation given here is that each DRE machines in every precinct should be connected to a device for independent verification. The reason for this

recommendation is that, if only some precincts are instrumented and a problem is found, the remaining precincts that have not been instrumented cannot be reviewed properly. The data necessary for independent verification would not have been collected. This situation does not apply for ballot-using systems, as the ballots not previously recounted remain available.

## 12. Recommendations

Audit of Election Results is Essential for Public Confidence: Thomas Jefferson's statement in the Declaration of Independence calling for "just powers from the consent of the governed" has been implemented in elections by the federal and state governments of this nation. Americans should be proud of the continuing use of elections over more than 200 years to peacefully transfer political power, even though it has been a long-term struggle to eliminate restrictions on the franchise due to property ownership, income, gender, and race. If elections are not carried out fairly, just powers cannot be expected, and the people lose faith in the democratic process. Public confidence requires that proofs be presented that elections have been carried out with integrity. The undertaking of audits will contribute significantly to that assurance.

If the numerical results of elections were in dollars rather than in votes, there would be no question that audits would have been carried out already for many years as a matter of course. Every corporation in the United States undertakes yearly audits as standard practice, in order to give investors, regulators, and taxing authorities a true understanding of the financial condition of the organization. There is no reason that elections should not undergo the same scrutiny. Assurance of integrity in the democratic process is at least as important as determining the actual financial state of a private firm.

The generation and retention of audit trails as an essential component of election equipment and the utilization of these data to actually conduct audits will significantly reduce the importance of vulnerabilities in computer security.

The Lack of Audit Trails Exposes Elections to Widespread Doubts: DRE voting equipment without independent verification requires correct software and faultlessly operating hardware in order to produce correct results. While election authorities in states such as Georgia and Maryland have gone to great lengths to assure that their voting equipment maintains integrity, they are constantly on the defensive. Computer scientists assert that software cannot be proven to be correct and some of them are continually finding computer security vulnerabilities that they make sure are widely publicized. At the same time, conspiracy theorists and losing candidates often use DRE machines without audit trails as a convenient excuse for election losses. Public confidence in the correctness of reported election outcomes has suffered.

The Paper-Trail Implementation is a Stop-Gap, Not a Permanent Solution: Several unacceptable attributes of paper trails are summarized here:

(1) Sighted voters can read the paper trail and validate their choices, whereas visually handicapped voters cannot carry out this task. Consequently, there are complaints that blind

voters do not have equal access to independent voting and, according to representatives of the disability community, this situation is a violation of HAVA.

(2) The verification of choices through the paper trail increases the time to vote, a frustrating condition to voters.

(3) Many voters are not verifying their choices with the paper trail because of the additional time required. Furthermore, many of those who make an attempt to verify are not reading their entire printout, as it is not presented in a human-friendly format and is presented in a different arrangement than on the electronic screen.

(4) There is a potential loss of privacy in use of the paper trail, as the printouts are rolled up for each machine in the same sequence as voters used it. Additionally, a voter who discovers a discrepancy between the printout and the electronic screen must lose his or her privacy in order to make that fact known.

(5) No IVD is being used now to obtain paper trail sums. Any independent verification must be done manually, summing the data from all of the printouts for each candidate on the ballot.

Requirements for an Electronic IVD: Products that can implement independent audit trails without a requirement for the voter to read a piece of paper have been discussed in Section 10. The opinions of this researcher on the performance requirements of such a product are as follows:

(1) The IVD must not provide a sighted voter with an advantage over a visually handicapped voter during the voting process.

(2) The electrical connection to a DRE from an IVD should be able to be simply accomplished and require, preferably, no modification of the DRE in hardware or software.

(3) During voting, the voter should not be required to perform any tasks on the IVD. This arrangement will prevent the addition of any time to voting and will not require the voter to learn new tasks. To provide assurance to the voter that his or her votes were received for counting, the IVD could be caused to print out, after the voter completes voting, a stub to be taken by the voter with a printed statement such as "You have voted," or the IVD could speak those words.

(4) The comparison of DRE and IVD results should occur after the close of polls. It is probably correct that the examination of the comparison of the DRE results with the IVD results that occurs after the polls are closed, undertaken by poll workers or election judges, does not require equal opportunity for the blind voter.

(5) The output of the IVD after the close of polls should include exactly the same set of results produced by the DRE so that they may be compared on a one-to-one basis. The IVD should be able to retain the final selections of each individual voter as well as the sums of votes for each candidate. The IVD output should be in digital form and may be on paper and/or on magnetic media, at the option of the user.

(6) The presence of "confirm" and "reject" buttons on the IVD are unnecessary. The voter will have already accomplished those actions on the DRE, and the function of the IVD is to assure that the DRE machine actually correctly records those choices and adds them correctly to the running sums of total candidate votes.

(7) The use of cryptography in an IVD, involving key distribution to encode and decode votes, is an unnecessary complexity that will confuse the voters and deter transparency. No

objection is envisaged to use of digital signatures to protect data or software integrity.

(8) Of the devices discussed in Section 10, VoteGuard from Democracy Systems is the only one apparently having the requirements enunciated here. It does not require any input from the voter, it does not provide sighted voters an advantage over blind voters during voting, it is easily connected to a DRE, it does not use key-based cryptography, and the results from the device are in digital form. This evaluation is preliminary; the device has not been examined in detail by this researcher and there may be competing devices not yet reviewed.

(9) If an IVD contains digital data processing capability, the manufacturer must agree that the software will be made public for purposes of scrutiny before it can be used. (The software may still be copyrighted.) IVDs must go through the VSTL process. Any financial or working relationship between the manufacturer of an IVD and the manufacturer of any DRE must be examined prior to the use of the IVD to assure independence.

Independent Verification of Voting Systems Using Hard-Copy Ballots: Voting systems using hard-copy ballots should not be exempt from a requirement to have an audit performed. It is often said, to distinguish ballot-based systems from DREs, that the ballots of the former are available to be recounted. However, they rarely are recounted, unless a defeated candidate pays for a complete audit of the ballots of the entire jurisdiction holding the election, as in Washington state's 2004 governor's contest. It has been pointed out that California has mandated a 1% recount of all ballots automatically without payment from a candidate, but that Ohio in 2004 undertook a 3% recount with payment required. In general, partial recounts are not undertaken automatically.

While concerns for lack of software correctness have driven the demands for audit trails for DRE voting machines, the question of actual recounting for systems employing hard-copy ballots has been ignored for many years. Nevertheless, there is some likelihood of degraded or incorrect sensing hardware for the counting of hard-copy ballots, and there is some likelihood of incorrect software generating wrong sums. A type of error sometimes seen, in the specialization process for an election, is that candidate A is assigned to receive candidate B's totals and vice-versa. This error is usually unintentional but, conceivably, it could be malicious. Thus, it is reasonable to require a partial recount of hard-copy ballots, automatically without payment by a candidate.

Based on the analysis discussed in Section 11, a partial manual recount of at least 3% should be undertaken. With software testing now being accomplished by the VSTL, and with adequate protection of this software in transportation and use, a 3% to 5% recount should be sufficient. It is important that candidates and parties be given the opportunity to select particular precincts, given local politicians' knowledge of expected results in particular areas. However, if an independently managed computer system is available, a considerably larger recount percentage could be used. The recounting of ballots on the same computer system as was used for the original count (a suggestion offered by unknowing election administrators in the past) will assuredly give the same answers as the first count, if no alteration to the computer program or review of the sensing capability, was undertaken in the mean time.

**References**


Bergholz, Richard, 1969, "Experts' Game: How Elections Can Be Rigged Via Computers," *Los Angeles Times*, July 8, p. 1.

Brace, Kimball W., 2004, Overview of Voting Equipment Usage in the Usage in the United States, Direct Recording Electronic (DRE) Voting, Election Data Services, Inc., Wash., DC.

Brennan Center Task Force on Voting System Security, 2006, The Machinery of Democracy: Protecting Elections in an Electronic World, The Brennan Center for Justice at NYU School of Law, New York.

Campbell, Tracy, 2005, Deliver the Vote: A History of Election Fraud, An American Political Tradition – 1742 - 2004, Carroll & Graff Publishers, New York.

Center for American Politics and Citizenship, 2006, A Study of Vote Verification Technology Conducted for the Maryland State Board of Elections, Part II: Usability Study, University of Maryland, College Park, MD.

Goldberg, Robert, 1987, "Election Fraud: An American Vice," in A. James Reichley (ed.), Elections American Style, The Brookings Institution, Washington, DC.

Kohno, Tadayoshi, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, 2003, Analysis of an Electronic Voting System, Technical Report TR-2003-19, Johns Hopkins University Information Security Institute, Baltimore, MD.

Norris, Donald F., Andrew Sears, and Charles Nicholas, 2006, A Study of Vote Verification Technologies, Part I: Technical Study, National Center for the Study of Elections of the Maryland Institute for Policy Analysis & Research, University of Maryland, Baltimore County, Catonsville, MD

Saltman, Roy G., 1975, Effective Use of Computing Technology in Vote-Tallying, Report NBSIR 75-687 (republished as NBS Special Publication 500-30, 1978), National Institute of Standards and Technology, Gaithersburg, MD.

Saltman, Roy G., 1988, Accuracy, Integrity, and Security in Computerized Vote-Tallying, NBS Special Publication 500-158, National Institute of Standards and Technology, Gaithersburg, MD.

Saltman, Roy G., 2006, The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence, Palgrave Macmillan, New York.

Selker, Ted and John Goler, 2004, Security Vulnerabilities and Problems with VVPT, Caltech/ MIT Voting Tech. Project, MIT, Cambridge, MA. [www.caltech.edu/Reports/vtp.wp13.pdf]