Statement of Barbara Simons for the Committee on House Administration Hearing on Electronic Voting Machines
September 28, 2006

My name is Barbara Simons. I am retired from IBM, where I was a Research Staff Member at the IBM Almaden Research Center for many years. I have been working almost exclusively on voting technology issues since 2000, when I was a member of the National Workshop on Internet Voting. The workshop, convened at the request of President Clinton, produced a report in 2001 in which we strongly recommended against Internet Voting. I also participated on the Security Peer Review Group for the US Department of Defense's Internet voting project (SERVE) and co-authored the report that led to the cancellation of SERVE because of security concerns. More recently I co-chaired the Association for Computing Machinery (ACM) study of statewide databases of registered voters. I am also co-authoring with Professor Doug Jones a book on voting machines to be published in 2007 by PoliPoint.

I was President of ACM from July 1998 until June 2000. ACM is the oldest and largest scientific and educational society of computer professionals, with approximately 80,000 members. I founded ACM's US Public Policy Committee (USACM) in 1993 and have served for many years as the Chair or co-Chair of USACM.

We must make our elections more secure, reliable, accessible, and verifiable.

We all want elections that are reliable, secure, accessible, and trusted by the public. Given known security risks, the possibility that software bugs could generate incorrect election results, or that computerized voting machines may fail during an election, we cannot trust that the results recorded in a paperless voting machine accurately reflect the will of the voters. Providing a voter verified paper trail is a significant step toward mitigating these risks, restoring transparency to the election, and ensuring the public's trust.

Because paperless Direct Recording Electronic (DRE) devices cannot be audited, many states have mandated that DREs produce a voter verified paper audit trail (VVPAT) or voter verified paper ballot (VVPB). We have seen that careful and well engineered implementation of this requirement is critical. Some of the most widely used DREs have retrofitted their machines by adding reel-to-reel thermal printers. Unfortunately, there have been a number of problems with these continuous roll printers, including jamming, privacy concerns, and difficulties conducting a manual count of the paper.

There are high quality printers that are much more reliable, that produce easy to read text, and that could print VVPBs that are easy to count manually. Our voting systems should not depend on mediocre equipment.

Precinct based optical scan voting systems also produce VVPBs, since by definition the optical scan ballot is verified by the voter when he or she marks the ballot. Accessible

optical scan ballots can be produced using tactile ballots or electronic ballot marking systems. Optical scan ballots can be manually counted and used to audit elections.

As a defense against malicious or buggy software, we must have:

- reliable, well engineered, accessible VVPBs;
- policies and procedures that guarantee the integrity of the paper, control of custody, legibility, etc.; and
- routine mandated random manual audits of the VVPBs that instill voter confidence and that verify the accuracy of elections.

If the manual count does not match the count produced by an optical scan system or by a DRE, then all of the paper ballots must be manually counted in an open and transparent fashion. Unless there is evidence that the VVPBs have been compromised, the paper ballots should be used to determine the election results.

We can consider alternatives, such as cryptographic based systems, if and when voting technology is commercially available that is demonstrably secure, reliable, easy to use, accessible, believable, and understandable to the average voter.

Most computer professionals oppose paperless voting machines.

Computer scientists have been generally skeptical about computerized voting machines, because we know that they are not transparent. You cannot simply look inside a machine and clearly see if it is performing in a trustworthy manner. Computerized voting has a lot of advantages, but all computerized voting systems currently available carry risks. We recommend VVPATs or VVPBs not to eliminate fraud, but rather to increase the safety of voting systems and to allow for routine election audits.

Two years ago ACM issued the following statement[1] calling for well engineered voting machines that provide every voter with the ability to verify that his or her vote has been accurately cast by inspecting a physical (e.g. paper) record.

ACM Statement on E-voting

Virtually all voting systems in use today (punch-cards, lever machines, hand counted paper ballots, etc.) are subject to fraud and error, including electronic voting systems, which are not without their own risks and vulnerabilities. In particular, many electronic voting systems have been evaluated by independent, generally-recognized experts and have been found to be poorly designed; developed using inferior software engineering processes; designed without (or with very limited) external audit capabilities; intended for operation without obvious protective measures; and deployed without rigorous, scientifically-designed testing.

To protect the accuracy and impartiality of the electoral process, ACM recommends that all voting systems – particularly computer-based electronic voting systems – embody careful engineering, strong safeguards, and rigorous testing in both their design and

operation. In addition, voting systems should enable each voter to inspect a physical (e.g., paper) record to verify that his or her vote has been accurately cast and to serve as an independent check on the result produced and stored by the system. Making those records permanent (i.e., not based solely in computer memory) provides a means by which an accurate recount may be conducted. Ensuring the reliability, security, and verifiability of public elections is fundamental to a stable democracy. Convenience and speed of vote counting are no substitute for accuracy of results and trust in the process by the electorate.

The League of Women Voters' resolution on voting systems.

In addition to the technical community, good government organizations have expressed concerns about the security of paperless voting machines. For example, at its 2006 national convention the League of Women Voters passed a resolution on voting machines calling for a voter verified paper ballot or record that would be used for audits and recounts. The League also urged that routine random audits of these paper ballots/records be conducted in every election. Here is the resolution[2]:

Whereas: Some LWVs have had difficulty applying the SARA Resolution (Secure, Accurate, Recountable and Accessible) passed at the last Convention, and
Whereas: Paperless electronic voting systems are not inherently secure, can malfunction, and do not provide a recountable audit trail,
Therefore be it resolved that:
The position on the Citizens' Right to Vote be interpreted to affirm that LWVUS supports only voting systems that are designed so that:

1. they employ a voter-verifiable paper ballot or other paper record, said paper being the official record of the voter's intent; and
2. the voter can verify, either by eye or with the aid of suitable devices for those who have impaired vision, that the paper ballot/record accurately reflects his or her intent; and
3. such verification takes place while the voter is still in the process of voting; and
4. the paper ballot/record is used for audits and recounts; and
5. the vote totals can be verified by an independent hand count of the paper ballot/record; and
6. routine audits of the paper ballot/record in randomly selected precincts can be conducted in every election, and the results published by the jurisdiction.

Insecure storage and handling of voting machines.

Professor Ed Felten, who is testifying today, recently released a very important study of fundamental security vulnerabilities of Diebold TS machines. The study illustrated how having physical access to one of the machines for even a minute was sufficient to allow a malicious individual to install fraudulent software.

There already has been a fair amount of press about the risks of voting machine "sleep-overs." This practice involves having a poll worker take a machine home prior to the election and bringing it in on Election Day. Decentralizing the physical security of machines significantly increases the number of people with access to a machine before an election. But even if machines are not delivered to poll workers' homes, there still can be significant security threats stemming from pre-election deliveries of machines, as I observed while serving as a Santa Clara County polling station inspector in the November 2004 election.

The county delivered five paperless DREs to our polling station – a commons room in a Stanford University dorm – about a week before Election Day. When the woman who made the space available for the election arrived at work, she moved the machines from the insecure commons room into her office, where they remained under lock and key until the night before the election.

My fellow poll workers and I set up the voting machines in the public commons room the night before the election so that the batteries could be fully charged. For the rest of the night the machines remained unattended.

When initially delivered, the machines were "protected" by two levels of numbered tamper evident tape. The first level was removed the night before the election, when we did the initial set-up. The second level was removed on Election Day. All of the removed tapes were included in the material that we returned to the county election officials.

I had no idea before the election as to what the tamper evident tape should look like, because I had never seen any. Even if I had been shown a tape, without additional training I doubt that my memory would have been adequate for me to know if a counterfeit tape had been used.

Security risks of the procedures deployed by Santa Clara County.

There are multiple security risks, depending on the goal of the attacker. Here are a few:

1. Hacking the voting machine software without being detected. This could have been done either by someone who had access to the machines while in the commons room, or by someone who had access to the office where the machines were stored. To avoid detection with certainty, it would have been necessary to acquire identically numbered tamper evident tape, for example by ordering it on the Internet or obtaining it from an insider working for the county.
2. Hacking the voting machine software and risking detection. Since we poll workers had never seen the tamper evident tape and had no idea of what the numbers on the pieces of tape should be, we would not have been able to determine that someone had hacked the software and replaced the original tapes with different tamper evident tapes. Such an attack might have been detected by election officials if they had reviewed the tapes that we returned. However, since

the election would have been over, it's not clear what election officials would have done. Furthermore, if the attacker had acquired identical or nearly identical tape and used the numbers from the original tapes on the counterfeit tapes, it's likely that even diligent election officials would not have detected the fraud.

3. Targeting specific precincts to depress turnout favorable to one candidate (a denial of service attack). This would have been a very easy attack, since the machines were left in a publicly accessible location the night before the election. All the attacker had to do was to remove the second level of tamper evident tape, since poll workers had been instructed to request new voting machines if the tamper evident tapes had been removed. Since we were barely ready by opening time, bringing in new machines would have delayed the opening of the polling station by at least an hour or two. If there were a widespread attack that removed the tamper evident tape from machines in many voting places, it is highly likely that the county would have been incapable of replacing all of the suspect machines.

Fortunately, there is a possible fix if tampering has been detected or there is a denial of service attack, namely emergency paper ballots. Every polling place should have a large supply of emergency paper ballots that can be used in emergency situations. Furthermore, a manual count should be made of the emergency paper ballots in all suspect polling places **in addition to** any manual counts that are done to satisfy a random manual audit.

Voters with disabilities.

While HAVA was passed in response to problems with the 2000 elections, much emphasis has been given to the HAVA requirement that voting be made accessible for people with disabilities. However, security and accessibility are not mutually exclusive goals. We can and should have secure accessible elections.

I cannot stress enough that I strongly agree that people with disabilities should be able to vote privately and independently and that they should be able to verify their votes. I do not know a single computer security expert who opposes non-visual access for blind voters or access to the ballot by any person with a disability.

It bears repeating that HAVA does not mandate the exclusive use of electronic voting machines to meet accessibility requirements. HAVA states accessibility can be met "…through the use of at least one direct recording electronic voting system *or other voting system equipped for individuals with disabilities…*" [emphasis added].[3]

There is a growing body of evidence that people with disabilities - blind and visually impaired voters, voters who have limited mobility and dexterity, and people with other disabilities - are finding that DREs or touchscreens are not meeting their accessibility needs and are in fact preventing them from securing a private and independent ballot.

Aleda J. Devies, a retired systems engineer, and member of Handicapped Voters of Volusia County, made the following statements in her August 01, 2006 article, *Touch Screens Are Not The Best Choice For Disabled Voters*:[4]

A key point has been lost in the various arguments for and against touch-screen voting machines. The spirit and intent of the accessible voting law are to allow every disabled person the opportunity to cast his or her [sic] privately and independently. The key word in the preceding sentence is "every." It is not acceptable to accommodate some members of the disabled population and expect the rest of us to live with "business as usual." That is discrimination, which is not legal.

Accommodating people with different disabilities requires great flexibility in a voting system. What works for and is preferred by certain members of the blind and visually impaired community does not accommodate people with mobility or motor impairments. That is one specific shortcoming with touch screen machines. People with limited use of their hands and arms may not be able to use the touch screen machines. People with spinal cord injuries or similar disorders may require binary devices such as such as "sip-and-puff". (Other binary devices include foot pedals, joy-sticks and gel pads.)

Devies also observes that, "Touch screen machines with telephone-like keypads do not meet Section 508 of the Rehabilitation Act of 1973 requirement that keypads must be operable with one hand and shall not require tight grasping, pinching, or twisting of the wrist."

Kelly Pierce, a nationally-known advocate for people who are blind and visually impaired, reviewed four voting machines in his March 15, 2005 report for the Cook County State's Attorney's Office, *Accessibility Analysis of Four Proposed Voting Machines*.[5]

Pierce analyzed tactilely discernable controls, spoken prompts, visual display, poll worker assistance, volume control and normalization, and ballot review. He found all four machines deficient in one or another of these areas.

Pierce stated, "Unfortunately, if any one of the four machines were to be deployed in Chicago or suburban Cook County as exhibited on March 15, many voters with disabilities, particularly blind voters, would not be able to cast a ballot independently and privately".

In his conclusion, Pierce remarks, "This review and those conducted by the American Foundation for the Blind, Manhattan Borough President C. Virginia Fields with The Center for Independence of the Disabled in New York, and a blind computer scientist and electrical engineer all have found that while the electronic machines represent a significant advance in accessibility from the current poll worker assistance system they often fail to effectively communicate the voting process to audio voters or are physically designed in a way that does not meet the current consensus on accessible design as

crafted by the technology industry, the disability community, and leading national governmental institutions."

Pierce's observations appear to have been born out by the voting experience of Noel Runyan, a blind computer scientist. Runyan, who has worked in human factors for well over thirty-five years, started his own company to supply access technologies for the visually impaired. Quoting just a small portion of Runyan's essay in frustration from his 65 minute voting experience in the 2004 Presidential election:[6]

It took me 30 minutes to work my way through the ballots and make my selections. After that, I had quite a bit of trouble getting into the review mode, to get a full list of all my selections. When I did, it went on and on, for 23 minutes, like a long uncontrolled drink from a fire hose. The review function read each item, and then, at the very end, said what my selection was for that item. It even threw in the details of what the fiscal impact would be, and took forever. This is completely backwards. It should announce the name of the item, then state my selection, and then read the rest of the information for that item. Also, I should have the control to press the arrow key to move forward or backward through the items, without having to listen to all the text about an item.

When I did find that I had made a mistake in my selections, I had to wait until the end of the whole review process to correct it, instead of being able to stop, make the change, and then continue with the review where I left off.

I did not want to abort the ballot verification review, to make a correction, and then have to start the 23 minute review all over again. When I later attempted to change one of my selections from "no" to "yes", the machine would not let me just select "yes", until I had first gone to the "no" entry and deselected it. This was very awkward and confusing. My wife said that she also had the problem when she was voting visually on her DRE machine.

Blind and disabled voters want and deserve secure voting systems. Natalie Wormeli, a lawyer who is completely blind, has manual dexterity issues, and uses a wheelchair[7], is far more eloquent than I could ever hope to be in her in her 2004 testimony before the California State Senate Elections and Reapportionment Committee, :

I deeply regret that I am unable to testify in person at today's hearing because of serious health problems. Please consider the following as my written testimony. I am writing this letter as a concerned California voter, an attorney, and a woman with multiple disabilities. For purposes of this letter, I am only representing myself, and I do not claim to speak for anyone else.
…
I am particularly offended by the reoccurring claim that people with disabilities are disenfranchised. This is highly inflammatory rhetoric, ignoring the definition of enfranchisement, which is a person's right to vote. When I turned 18, I became enfranchised. Not having the ability to vote without another human being's assistance is the reality that I deal with, but does not make me disenfranchised. I rely on other people

to help me with tasks that I am not physically able to do, but I remain in control and independently thinking the entire time. When voting, I can choose to bring a friend, a family member, or ask one of the well-trained poll workers for assistance.
…
Providing flawed DRE systems would erode trust among voters with disabilities as well as able-bodied voters in California and throughout the country. If Californians depend on flawed systems, and California has problems in November, the headlines throughout the country will undoubtedly reflect this horrible fact.

Other disability rights advocates claim that decertification would be a step back, treating people with disabilities as second class citizens. I argue that requiring California voters to use dangerously flawed DREs will be forcing second rate technology on us all.

I know that DRE system developers are working tirelessly to create dependable secure systems, and I am confident that one day I will be able to vote privately without assistance. However, I refuse to act as a complaining passenger in the backseat asking, are we there yet? I know I will be there soon enough, but I only want to arrive safely and with everyone on board. I know that when SB 1723[8] is passed, you will be heroes for all the citizens of California, especially voters with disabilities.[9]

For many people with disabilities, using a VVPB presents no accessibility difficulties whatsoever and does not in any way prohibit private and independent voting. Fortunately, we do not have to settle for voter verified paper ballots that are not accessible to blind and visually impaired voters. It is not difficult to integrate audio capabilities into the design stage of voting systems. Tactile ballots and tactile voting systems allow blind voters to vote privately and independently and to verify their votes. New technologies can and should be developed. For example, hand held text-to-speech reading devices, such as the one recently announced by the National Federation of the Blind, might be modified for use in elections.[10]

It's time for us to demand of our voting systems that, in addition to being accessible, they must be safe, accurate, reliable, secure, and audited. For now that means that we need voter verified paper ballots, routine random manual audits, improved policies and procedures, increased transparency, and a national mandate that voter verified paper ballots shall be the official ballots used and the final authority in all cases of recounts, challenges, random manual audits, equipment malfunction, and suspect polling places. As President Reagan said: Trust, but verify.

It is part of our nature to rely on technology to improve our institutions. Voting and voter registration are no different. Technology, if engineered and tested carefully and if deployed with safeguards against failure, can reduce error rates, provide more accessibility, increase accountability, and strengthen our voting system. However, we have rushed to put technologies in place without careful regard as to how they must perform. We are now seeing questions raised about the security, reliability, accessibility, and usability of these machines. We can take immediate steps to address security concerns by ensuring that we have voter verified paper ballots and routine random

manual audits. Beyond this, the technical community and the election community need to work together to develop computerized voting and electronic registration systems that truly deserve the public's trust.

Appendix: Electronic Voter Registration Databases

While beyond the scope of this hearing, we are seeing serious problems with statewide electronic voter registration databases. One of HAVA's key provisions requires all states to have statewide electronic databases in place by the beginning of this year. Some states already had these systems in place; others were faced with difficult decisions on how to consolidate or synchronize disparate local databases into a statewide system. Like all technology, these systems are complex and require careful engineering so that they are accurate, private, secure, usable, and reliable. Otherwise, voters can be rejected at the polls and disenfranchised, or the systems could be exposed to fraud from unauthorized access. USACM released a study earlier this year[11] that provides 99 recommendations for state and local officials to follow when implementing electronic voter registration databases.

---

[1] http://www.acm.org/usacm/Issues/EVoting.htm

[2] http://www.lwv.org/AM/Template.cfm?Section=Reports_from_Convention&Template=/MembersOnly.cfm&ContentID=5597

[3] http://www.fec.gov/hava/law_ext.txt

[4] http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1595&Itemid=26

[5] http://www.votersunite.org/info/KellyPierceReport3-05.htm

[6] *Voting experience in November 2004 Election in Santa Clara County California – Using Sequoia Voting Machines*, by Noel Runyan, http://www.votersunite.org/info/RunyanOnSequoia.htm

[7] Wormeli's description of herself given in testimony at the Meeting of the State of California Secretary of State Voting Systems and Procedures Panel, April 28, 2004, Sacramento, CA., http://www.ss.ca.gov/elections/vsptranscript0428.pdf

[8] SB 1723, which would have required that all voting machines produce an Accessible Voter Verified Paper Audit Trail (AVVPAT) by some deadline. Later in 2004 SB 1438, which essentially prohibited the deployment of voting machines that did not produce an AVVPAT by 2006, became law.

[9] Testimony before the California State Senate Elections and Reapportionment Committee, by Natalie Wormeli, Esq., May 5, 2004. Wormeli's complete written testimony can be found at http://www.wheresthepaper.org/NatalieWormeli.htm or http://www.leagueissues.org/cdrom/disabled/Security.doc.

[10] *The Kurzweil-National Federation of the Blind Reader: The Revolution* Is Here!, by James Gashel, http://www.nfb.org/Images/nfb/Publications/bm/bm06/bm0607/bm060703.htm

[11] *Statewide Databases of Registered Voters: Study of Accuracy, Privacy, Usability, Security, and Reliability Issues,* February, 2006, www.acm.org/usacm/vrd.