A Response To:

THE LEAGUE OF WOMEN VOTERS OF THE UNITED STATES

Questions and Answers on Direct Recording Electronic (DRE) Voting Systems

Dr. Barbara Simons
Past-President Association for Computing Machinery
Member, League of Women Voters of Palo Alto, California

Executive Summary.

The Q & A written by the League of Women Voters of the United States (LWVUS) and posted on their website contains a number of inaccuracies and omissions. Regrettably for the good name of the LWVUS, the Q & A is being widely distributed. It is even being used by the LWVUS to lobby one or more co-sponsors of H.R. 2239 - legislation aimed at making computerized voting machines secure through the use of voter verified paper ballots - in an effort to get them to withdraw their sponsorship.

Here are some of the claims made by the LWVUS that we rebut:

- *We can trust the software that runs paperless Direct Electronic Recording (DRE) voting machines.*
  This claim ignores the many problems that have been repeatedly pointed out by computer scientists, such as software errors (bugs) and malicious code that could be inserted by a vendor employee or a non-employee who gains access to the software.

- *We can trust the testing and certification of DREs.*
  There are no grounds for such trust, as we have seen with the multitude of problems that have occurred with DREs. Furthermore, there are sound technical reasons for why even good software testing, which we don't currently have for DREs, is bound to fail.

- *We cannot count paper.*
  This conclusion is obviously erroneous, as paper is accurately counted throughout our society, for example by banks, and in national elections of many other democracies.

- *Voter Verified Paper Ballots discriminate against the visually impaired.*
  The LWVUS sometimes claims that the voter will be required to verify his or her ballot, which is simply untrue. Furthermore, there are technologies that currently exist that allow a blind voter to verify his or her paper ballot.

- *Printers for Voter Verified Paper Ballots are too expensive and are likely to break down.*
  [We note that optical scan ballots are cheaper than DREs, are voter verified, and do not require printers]. Ironically, DREs already come with printers that print out so-called ballot images at the end of an election. If touch screen voting machines had been better designed to begin with, they could have had printers that would print out a voter verified paper ballot at the time that the voter actually casts his or her vote. In addition, we know how to build highly reliable printers that are very unlikely to break down, though retrofitting current DREs or replacing them with secure and reliable machines will cost money. Ultimately, we must ask how much our democracy is worth. The founders of the LWV suffered and went to jail in their fight for universal suffrage. Prior to and during the Civil Rights Movement African Americans were murdered in the struggle for the right to vote. Does the LWVUS now argue that we cannot afford the additional cost of reliable printers to safeguard our vote?

In summary, there is no way to know in an election using paperless DREs whether or not the votes cast have been correctly recorded and counted.

The Response to the LWVUS Q & A.

QUESTION: What is the controversy over Direct Recording Electronic (DRE) voting systems?

LWVUS ANSWER: Some claim that electronic voting machines are subject to manipulation that will allow votes to be stolen, and that the only way to protect against this is to have a voter verified paper trail (VVPT). The concerns come in three areas. First, some say that a "Trojan Horse" computer chip or special code could be installed in the voting machine by the manufacturer or another "insider" that would cause votes to be incorrectly recorded. Second, some suggest that the machine could be penetrated ("hacked") or that the management security systems could be bypassed to allow an outsider to manipulate the voting machine. Finally, some observers are concerned that linking voting machines electronically or using the Internet to transmit election results will allow results to be manipulated.

MEMBER RESPONSE: The answer is incomplete. In addition to the risk of malicious software, there is a very serious risk that software errors (bugs) could result in an incorrect recording or tallying of the votes. Errors could easily go undetected since voters cannot inspect the electronic versions of their votes saved by the machine. Even detected errors can create problems if votes have already been lost. This happened in Wake County, North Carolina in November 2002, when ES&S machines did not count 436 ballots.

QUESTION: Is this something that I should worry about, as a voter?

LWVUS ANSWER: There is no reason to believe that a well-run election system based on DREs will steal your vote. In fact, modern voting systems like DREs and precinct-count optical scan voting systems can be much better than the punchcard voting machines and lever machines that they are replacing. At the same time, it is important that election officials put management safeguards in place to ensure that all voting systems function properly.

MEMBER RESPONSE: We agree that precinct-based optical scan voting machines are certainly better than some of the older voting machines, and they also provide voter verified paper ballots. By contrast, there is no way in an election using paperless DREs for you to know whether or not your vote has been correctly recorded and counted, even if the election is "well-run." Your vote could be stolen or simply incorrectly recorded or counted because of software bugs.

While we have no proof at this point that outright fraud has occurred, there is no proof that it hasn't. More importantly, there is no way to audit an election using paperless DREs if fraud is suspected.

QUESTION: Then why is there such a debate?

LWVUS ANSWER: The concern about electronic voting machines taps into deep reservoirs of distrust: distrust of the election systems that were so flawed in 2000, distrust of new technologies; and basic distrust of the political system. Many Americans became deeply concerned after the 2000 election revealed the problems that plague our election systems. “Hanging chads” were just part of the problem as Americans learned about such issues as voting machines that don’t work well, poor ballot design, and people being turned away from the polls because of poor administration of voter rolls, including erroneous purging. In addition, many people are uncomfortable with or distrustful of new technologies, even though we rely on such technologies to fly our airplanes and operate our banking systems so long as there are appropriate management systems to provide safeguards. Finally, computer specialists with limited experience with election systems have focused narrowly on the DRE machines themselves without taking into account the management systems and safeguards that can protect against tampering and without acknowledging the problems associated with other voting systems such as punchcard machines.

MEMBER RESPONSE: Concern about electronic voting machines stems from knowledge of how easy it is to hide malicious code within a large and complex piece of software. Finding such code is akin to finding the proverbial needle in a haystack. In addition, it is essentially impossible to write a large amount of complex code that is error-free. That is why the debate was initiated primarily by Ph.D. computer scientists - people who understand how computers work and who realize all too well that paperless DREs are extremely vulnerable. The very technology on which paperless DREs are based was developed by computer scientists. Comparing opponents of paperless DREs with people who are afraid to fly airplanes makes as much sense as calling computer scientists who oppose paperless DREs “Luddites,” as some defenders of paperless DREs have done.

Many of the problems and risks about which computer scientists are warning cannot be corrected even with good management systems and safeguards. Unfortunately, we have neither good management systems nor safeguards in place for the current crop of paperless DREs.

Furthermore, while several of the computer scientists who are raising the alarm against paperless DREs have extensive knowledge of and experience with election systems, such knowledge is not necessary if one is analyzing only problems relating to the computers that run the paperless DREs. To say otherwise is like saying that a researcher in lung diseases is not qualified to state that cigarettes can cause lung cancer because that researcher is not also an expert in arthritis.

QUESTION: What are DREs?

LWVUS ANSWER: Direct Recording Electronic (DRE) voting systems are one of two types of modern voting machines; the other is the precinct-count optical scan system. Both these systems are improvements over older systems such as punchcard machines, lever

machines, paper ballots, central-count optical scan machines and a previous generation of older computer machines. The DRE is also called a "touchscreen" voting machine or an electronic voting machine. The voter touches a computer screen to vote for each candidate or issue, has an opportunity to review the ballot, and then casts the ballot on the electronic machine.

MEMBER RESPONSE: A voter using a paperless DRE does not have an opportunity to review his or her ballot. The voter, seeing only a picture of the ballot on the touch screen, has no way of knowing if the screen image corresponds to the values that are recorded in the computer. It would not be difficult to program a DRE so that some of the votes are changed between when the voter "sees" his or her vote on the screen and when that vote is "written" in the computer.

But the voter need not trust a paperless touch-screen machine. Avante produced the first commercially available touch-screen voting machine to produce a voter-verified paper ballot, and others are being developed.

QUESTION: What are the advantages of DRE systems?

LWVUS ANSWER: There are a number of advantages to DRE systems. They can easily be adapted with earphones and other devices so that persons with disabilities can cast ballots independently and in private, and they are easily adapted for multiple languages. They directly record votes so they provide accurate counts, and there must be a paper record of all the votes cast on each voting system. DREs provide for "second chance" voting in private, so that a person who makes a mistake in voting can automatically be notified and make a correction to the ballot before it is cast. In the case of an "overvote," where a person mistakenly votes for more than one candidate for an office such a President, the machine can automatically prevent the error in the first place. Studies indicate a high degree of acceptance of DREs by voters, of all ages and ethnic and racial backgrounds, who have used them. DREs also reduce many of the operational problems in handling paper ballots that have sometimes led to election irregularities. As discussed in this document, there is controversy over the security of DRE machines.

MEMBER RESPONSE: The "paper record of all votes cast on each voting system" is nothing more than a print-out at the end of election day of the contents of the computer's memory. Such a printout is meaningless if the votes are not recorded correctly initially. In addition, second chance voting is of no value if the vote is not accurately recorded and counted by the DRE.

QUESTION: What are precinct-count optical scan voting machines?

LWVUS ANSWER: Optical scan machines use a ballot printed on special paper that is then marked by the voter, usually with a #2 pencil or with a special marker. The ballot is then fed into a counting machine that reflects light off the markings to scan and count the vote. Central-count optical scan systems, where the ballots are collected and sent to a central location before being scanned, cannot provide for "second

chance" voting, as is required by the Help America Vote Act (HAVA), because the voter cannot make a correction to the ballot. With precinct-count optical scan systems, the voter or an election official puts the ballot in the scanner at the polling place. If there is a problem, such as an "overvote," the scanner returns the ballot for correction by the voter. Central count is used for mail-in and absentee voting.

QUESTION: What are the advantages of precinct-count optical scan systems?

LWVUS ANSWER: There are a number of advantages and disadvantages for precinct-count optical scan machines. The initial costs of such systems are lower than for DREs, but the costs of printing the ballots on the special paper raise the costs over the long run. Because they are based on marking a paper ballot, persons with physical disabilities and those who are blind or have declining vision, such as the elderly, have trouble with these systems. In addition, the process for "second chance" voting is not private: if the scanner sees a problem, the election official returns the ballot to the voter, a potentially embarrassing and perhaps intimidating process. Localities with significant numbers of voters who would benefit from a ballot in a language other than English, but which are not required by federal law to offer such ballots in those languages because the number of such voters is not sufficiently large, will not offer ballots in multiple languages because of the costs of printing the ballots. The optical scan ballots can be recounted, but there have been reliability and repeatability concerns in some elections.

MEMBER RESPONSE: Costs for storage, security, maintenance, and precinct worker training also are significantly higher for DREs than for optical scan machines. (See the discussion of Miami-Dade below for a specific example). Furthermore, it is possible for people with impaired vision to have voter verified paper ballots while retaining all the advantages of touch screen voting machines, including "second chance" voting. For example, there is a touch screen optical scan ballot marking device manufactured by Vogue Election Systems that does not record votes internally but instead marks the optical scan ballot for the voter, thereby protecting against stray or ambiguous marks, as well as over votes.

As far as reliability is concerned, according to an assessment by Caltech and the MIT Voting Technology Project of recent presidential contests, DREs are less reliable than paper ballots. Punch cards had the highest uncounted rate at 2.5 percent, followed by electronic/touch screen voting at 2.3 percent, paper ballots at 1.8 percent, and optical scanners tying with lever machines for the best-in-show error rate of 1.5 percent
http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/09/21/IN146265.DTL.

QUESTION: What are some of the safeguards that can protect against a malfunctioning voting machine?

LWVUS ANSWER: Voting machines are scrutinized by state officials and computer specialists before a machine is certified for use in their states. Voting machines are also

tested to guard against malfunctions, and management systems guard against error and ensure that unauthorized personnel do not have access to the machines. Testing and monitoring typically occurs many times in well-run systems: First, voting machines must meet nationally certified design standards in most states. Second, the individual machines are tested when they are delivered by the manufacturer to election officials. Third, the machines are tested just before Election Day. Fourth, and especially important, the machines are monitored during Election Day. Finally, the machines are tested after Election Day. Security measures prevent tampering after each stage of the process. Each of these tests helps guard against the use of a malfunctioning machine, and, taken together, suggests a high degree of reliability. Of course, as with any system, if the safeguards are not followed, then problems can result.

MEMBER RESPONSE: It is unfortunate that the running of our national elections and the testing of the software operating on those machines are being handed over to a small handful of private organizations acting in secret. The tests might uncover certain types of machine malfunctions, but most of them do not even examine the software for errors, and therefore cannot determine if there is buggy or malicious software that could impact the election. For example, the ES&S machines that lost 436 ballots in Wake County, NC had been certified.

Furthermore, it is impossible to put security or reliability into software simply by testing. There are many other requirements relating both to the nature of the code (e.g. suspicious subroutines) and to the manner in which it was created (e.g. code inspections and version control).

Regarding the specific claims: First, the national certified design standards are totally inadequate in terms of guaranteeing that the voting machines will correctly record and count the votes. Certification testing is secret and the results are hidden from the public and from independent computer security experts.

Even if certification were adequate, we have seen a number of cases, such as all Diebold electronic voting machines used in California (17 counties in all), in which voting machines have been run using non-certified code. There are also reports of non-certified voting systems being used in Ohio and Florida.

Second, state officials and computer specialists learn very little about the security of the software that operates the voting machine by “scrutinizing” those machines. They must examine the actual software, just as a competent doctor would want to examine X-rays to determine the extent of internal injuries in the victim of an accident.

We know from a study of Diebold code that was insecurely stored on a publicly accessible Internet site http://avirubin.com/vote.pdf that the official testing is inadequate, the people doing the testing are most likely not computer security experts, and the testers do NOT analyze the logic of the software. (Diebold security problems have been independently verified by reports commissioned from Science Applications International Corporation (SAIC), Compuware, and RABA Technologies).

Consequently, hidden malicious code would almost certainly escape the attention of the testers. However, even if the testers were highly qualified, cleverly concealed malicious code would be extremely difficult to detect. Finding such code is akin to finding the proverbial needle in a haystack.

Third and fourth, testing the machines just before and during Election Day is meaningless if the tests themselves are meaningless. Finally, tests that help guard against obvious malfunctions of voting machines prove nothing about non-obvious or hidden malfunctioning. Even if all of the safeguards described by the LWVUS were to be followed, we would have no way of knowing whether or not the voting machines accurately recorded and counted the votes.

Facts not discussed by the LWVUS are:

1. Software (Commercial Off The Shelf, or COTS) used in commercial products that are utilized by voting machines is not examined. Yet, over 4000 COTS vulnerabilities were reported in 2000. An issue that the LWVUS has not discussed is how vendors can install "bug fixes" to COTS used in their systems and recertify the systems (this is supposed to be done whenever a change is made), given that bug fixes can be released monthly, weekly, or even daily. For example, in February, 2004, Microsoft released several important software patches, including one for a security vulnerability that is present in every unpatched copy of Windows NT, Windows 2000, Windows XP, and Windows Server 2003.

2. Even if far more appropriate testing were done, some software bugs would go undetected. This is because of the fundamental problem that software of any significant size is very complex, and computer programmers are unable to write error-free code. Major software vendors such as Microsoft who devote vast sums of money to correcting software bugs nonetheless are forced to issue frequent bug fixes.

3. It is very difficult to detect malicious code that is cleverly hidden in software. For example, a full-fledged flight simulator was initially undetected in Microsoft's Excel 97 spreadsheet application. Furthermore, the lead author of the SAIC report, Frank Schugar, in testimony before the Maryland House Ways and Means Committee on Nov 13, 2003 about Diebold software, said that a security audit would almost certainly fail to detect a carefully planted bit of malicious code intended to fix elections.

QUESTION: But I have heard that you can't test a machine in operation, only in "test mode." What protects against a "Trojan Horse" computer chip or code that a manufacturer or other insider might put in a machine? Couldn't it be programmed only to manipulate the vote on Election Day, and not be active at any other time?

LWVUS ANSWER: Voting machines can be tested in "election" mode. Not only can the tests be designed to simulate the specific conditions under which the machines will be used on Election Day, the internal clock on the machine can be adjusted to assure that

the machine "thinks" it is running in real time on Election Day, when it is, in fact, being tested. Some have suggested that the "Trojan Horse" could contain its own clock or other mechanism that would activate only on the real Election Day and that it could bypass the testing. However, computer specialists point to testing and monitoring on Election Day as an additional safeguard against this scenario. The best tests include randomly taking a machine out of service to run "test votes" to verify accuracy. This should be done with people from all interests represented. Since current voting machines do not use special technology to guard against external break-ins, one key safeguard is to ensure that voting machines are not linked together, or linked on the Internet, because such connections could allow rogue programs to penetrate the system after testing.

MEMBER RESPONSE: It is not clear what the LWVUS means by "election" mode. Not only should all internal clocks be reset to the date of the election (and the machine unable to detect that the clocks had been reset), but also the testing should simulate the way things happen on Election Day. The votes would have to be entered manually during the number of hours that voting would take place. Also, the manual entries would have to be meticulously recorded and executed, since a slight variation in the expected results could be attributed to faulty record keeping or vote entries.

In reality, the way that most testing is done would allow a clever programmer to write code to detect that testing is occurring. Almost all testing involves at least some automatic (not manual) entry of test votes over a far shorter time period than the length of the election. And clocks frequently are not reset.

While the best testing would involve the simultaneous manual testing of a test voting machine on Election Day, this testing typically is not applied. For example, in a Feb. 10, 2004 letter written by ten California Registrars of Voters to the California Secretary of State Kevin Shelley in response to Shelley's request for "parallel monitoring" of paperless DREs, the registrars object to "an unspecified amount of expensive DRE equipment that our counties purchased for use by the voters on election day [being used] for this 'testing'."

In addition, the LWVUS does not say what it would recommend if Election Day testing were to turn up problems. If a test machine were to record and count votes inaccurately, then all machines would be suspect and the results of the election would be widely questioned. Would the LWVUS recommend rerunning the election? What legal provisions would allow an election to be rerun? How would anyone know that a rerun election conducted on the same machines would be any more reliable than the initial election? These are critical questions that the LWVUS has not addressed.

What would the LWVUS recommend when problems with DREs are detected during an election? For example, in a November, 2003 election in Houston, Texas, 12 eSlate voting machines were set up incorrectly. As a result, people who attempted to vote at the Holiday Inn at 7787 Katy Freeway were given scraps of paper on which to vote by election judges. As one person who spent 25 minutes sitting on the floor writing

down his choices said, “They’re making up rules as they go. It’s unbelievable.” [Quote taken from an article in the Houston Chronicle.]

QUESTION: What are the safeguards that protect against outside interference? Couldn’t a technologically adept voter vote several times?

LWVUS ANSWER: There are a variety of management safeguards to protect against outside interference. The most important ways are to ensure that voting machines are not linked together or linked on the Internet, and that results are not transferred directly from the machines over phone lines. Isolating each machine ensures that any possible problem with one machine does not contaminate the system as a whole, making it much more difficult to affect an election. Isolating machines from the Internet and from phone lines prevents entry into a voting system through those routes. Other safeguards include restricting physical access to machines and setting up polling place operations that monitor machine usage, including the number of votes being cast. To tamper with a DRE someone would need to know each of the security systems within the machine, including codes, formats and storage capacities, and be able to manipulate them undetected after first gaining sufficient access to spend the necessary time with the machine. DREs are not an election system unto themselves; they are simply an instrument within a complex election system. It is the interaction of the technical, physical, and procedural security measures that actually secure the voting system, not any one of these measures alone. The key is to have an overall system that builds in multiple checks making it improbable that the system will be tampered with.

MEMBER RESPONSE: Isolating machines is a good idea, and some of safeguards mentioned could help prevent an outsider from tampering with the machines, assuming that the safeguards are assiduously followed.

While the question addresses only the threat of outside interference, the far more significant threats are buggy software and manipulation by an insider. Since all voting machines of a particular type from the same manufacturer use identical software, malicious or faulty software could impact all of the machines used by a particular state - such as Georgia or Maryland. That means that not only the Presidential electoral votes could be incorrectly reported, but also the results of races for the Senate, House of Representatives, Governor, and lower level positions could be modified.

For example, there are people who question the reported outcome of the State of Georgia’s November 2002 election in which the entire state voted on Diebold machines. Because no paper ballots were produced in the election, there is no way for the state of Georgia to prove that the reported winners actually won the election.

While it's true that DREs are part of an overall system, they are a critical part. If DREs incorrectly record or count the votes, it doesn't matter what happens in the rest of the system. The reported results will not reflect the will of the voters.

QUESTION: I heard that the new Maryland voting system was challenged because of security concerns.

LWVUS ANSWER: The governor of Maryland ordered a review of Maryland's new DRE voting systems after a report from a professor at Johns Hopkins University suggested that security could be breached. The independent security analysis done for the state by Science Applications International Corporation (SAIC), an independent IT firm with an international reputation in IT security, found that DREs can work effectively, but, like all systems, need good management systems to ensure the reliability and integrity of the voting process. A number of recommendations were made, including isolating the system from any network connections, appointing a chief security officer, developing a formal set of policies and procedures through all jurisdictions, and creating a formal security plan using recognized "best practices." None of the recommendations by SAIC included the use of a voter verified paper trail (VVPT).

MEMBER RESPONSE: The SAIC report, which was heavily censored (a fact that appears not to disturb the LWVUS), contains the following quote:

"The system, as implemented in policy, procedure, and technology, is at high risk of compromise. Application of the listed mitigations will reduce the risk to the system. Any computerized voting system implemented using the present set of policies and procedures would require these same mitigations." page V, Executive Summary, SAIC report on Diebold.

The above quote does not guarantee that the Diebold machines will be safe and trustworthy, even if the "listed mitigations" were all to be implemented. In fact, SAIC issued the following disclaimer:

"SAIC cannot guarantee or assure that risks, vulnerabilities and threats other than those addressed in this report will not occur nor can we guarantee or assure that, even if the State of Maryland implements the recommendations we have proposed, the State's business, facilities, computer networks and systems, software, computer hardware and other tangible equipment and assets will not be compromised, damaged or destroyed." page 12.

Furthermore, quoting from "Voting security Debated" in
http://www.gazette.net/200346/weekend/a_section/187979-1.html

> In fact, in a Nov. 13, 2003 hearing by the State of Maryland House Ways and Means Committee, Frank Schugar, project manager for SAIC, praised Rubin's work [the Hopkins paper] and said he is "extremely well-versed and well-qualified and probably more so than I am personally."
>
> Schugar agreed with Rubin that someone could tamper with the program and that it would be "extremely difficult to detect," though not impossible.

> Schugar refused to answer when asked if the Diebold system passed muster. SAIC's job was to let the state know the risks it is taking. "Whether or not those risks are acceptable is a political decision," he said.

In other words, the SAIC report states that at best the recommendations would "reduce the risk to the system" and that they cannot guarantee even that. The manager for SAIC publicly praised the work done to reveal the insecurities in the Diebold code. This is hardly the ringing endorsement implied by the LWVUS.

In January 2004, a report on security problems with Maryland's Diebold machines was issued by RABA Technologies. RABA had been hired by Maryland to test the security of Diebold machines by attempting to break into (hack) them using a "Red Team." Quoting from a January 29, 2004 article in the New York Times:

> The authors of the report said that they had expected a higher degree of security in the design of the machines. "We were genuinely surprised at the basic level of the exploits" that allowed tampering, said Mr. Wertheimer, a former security expert for the National Security Agency.
>
> William A. Arbaugh, an assistant professor of computer science at the University of Maryland and a member of the Red Team exercise, said, "I can say with confidence that nobody looked at the system with an eye to security who understands security."
>
> The new report vindicates a controversial report that found Diebold software lacked the level of security necessary to safeguard the election process or even to meet the standard practices of the computing industry, and it underscores the results of two subsequent studies.

QUESTION: I heard that the voting machine computer codes are kept secret and that computer professionals are prohibited from working with the machines by copyright laws and other regulations. How can we be sure that voting machines work properly if outside testers cannot get into the systems? Don't we need "open codes" and to allow "reverse engineering" in order to test the security of voting machines?

LWVUS ANSWER: Computer experts, retained by election officials under confidentiality agreements, currently review and evaluate computer codes and systems in the testing and evaluation of voting systems. In addition, secrecy is an important security measure. Limiting access to computer codes in DREs is important in protecting the voting system. If those who might want to penetrate the system already know all the details of that system, it is much easier to breach security. "Open codes" can compromise security. However, it is vital that election officials have access to all design and other information about voting systems so that the machines can be certified, tested, and programmed with appropriate ballots. It is also important that responsible government officials and appropriate independent test authorities have reviewed the code and have control over the system, rather than relying on outside manufacturers or suppliers. As in any system, the expertise of managers and computer specialists is crucial in monitoring the practices of manufacturers and suppliers.

MEMBER RESPONSE: The notion that secrecy is an important security measure is referred to by computer scientists as "security through obscurity." It is well known to be antithetical to security. As we have learned from many years of study and experiment in the area of cryptography (the scrambling of messages), the very best kind of security involves making public the methodology being used (algorithms) and challenging the best minds to defeat the security. While we are unable to prove mathematically that any kind of computer-based security is invulnerable, the fact that very smart and talented people have been unable to "break" a particular kind of computer security (or cryptography) provides reassurance that the security is indeed strong.

The argument for "security through obscurity" rests on the reasonable assumption that there are security vulnerabilities in the source code, but draws the incorrect conclusion that the fewer people who know about them the better. This ignores the reality that a single individual with this knowledge might have the ability to fraudulently change the outcome of an election. Opening up the source code to inspection by a wide range of experts would greatly improve the chances of such vulnerabilities being identified before they are exploited.

QUESTION: Are election results transmitted over the Internet? Doesn't that allow the totals to be changed by a "hacker?"

LWVUS ANSWER: Most agree that connecting voting systems on-line substantially increases the risk that they can be penetrated. That's why well-managed systems are not kept on-line. Sometimes unofficial election results are transmitted over the Internet, but this should not be done directly from the voting machines. Security can be improved when transmittals are made at random times and are encrypted. More importantly, in well-run systems official results are computed directly from the memory cards and are not certified until they are double and triple checked with results that are not transmitted electronically.

MEMBER RESPONSE: The LWVUS has this one almost right. Random transmissions and encryption may help, but given the general insecurity of the Internet, voting results should never be transmitted over the Internet unless backup results are transmitted via a safer channel.

While results are recorded on memory cards, those cards themselves are a security risk. It is far easier to swap or discard a memory card, which is small, than it is to do similar things with a ballot box.

QUESTION: What is a voter verified paper trail or VVPT?

LWVUS ANSWER: A VVPT is an add-on system that prints out the voter's individual ballot choices after they have been cast on the DRE. Proponents of the voter verified paper trail argue that this allows the voter to confirm his or her votes and that it provides an opportunity for recounts since the paper record of each individual ballot is retained by election officials. The term is used interchangeably to refer to systems that simply provide the individual paper record and systems that would require that each voter actually verify the paper record of his or her vote.

MEMBER RESPONSE: None of the supporters of VVPT or Voter Verified Paper Ballots (VVPB) advocates requiring each voter to verify his or her paper ballot. Yet, elsewhere the LWVUS uses this claim to argue that blind voters would be discriminated against through the use of VVPB. This is simply untrue.

Most computer scientists are advocating a Voter Verified Paper Ballot, not Trail. The contents of

the DRE are at best an image of that ballot. And you don't need a DRE to have a VVPB. Optical scan ballots, for example, are by default voter verified.

Ideally, the VVPB would be the official ballot, and the results from the DREs would be only preliminary. At a minimum, some percentage of voting machines would be selected at random and all of the paper ballots generated by those machines would be manually counted. (California law requires a manual recount of 1% of the ballots, randomly selected). If the manual recount were to differ from the results reported by the machines, then all of the paper ballots would be manually recounted.

Better yet, the VVPBs would be printed in a form that could be read by optical scan machines. Then they would all be counted by the optical scanners, which should be manufactured by a different company from the one making the voting machines. And a small percentage of ballots would be manually recounted, as described above. In the event that any of the counts did not match, or in a close election, all of the paper ballots would be manually counted.

QUESTION: Why don't we require a voter verified paper trail as part of DRE voting machines? Won't having a paper record of every individual vote protect the integrity of the election system?

LWVUS ANSWER: There are a number of problems with requiring a voter verified paper trail as part of DREs. The most significant is that the VVPT does not provide a safeguard against the supposed problem: a machine that is programmed to record the incorrect vote. If the machine can be programmed to record the wrong vote, then it can be programmed to print out a misleading confirmation. Advocates say that the individual ballot paper confirmation can be recounted, to guard against this problem. However, a very important problem remains: The VVPT paper ballots are difficult, if not impossible, to recount consistently, leading to inaccuracies. The paper printed out from many of the add-on printers for DREs use script paper, like that in an ATM, or thermofax paper, like that in fax machine. It is not possible to recount that paper except by hand, a process that is extraordinarily cumbersome and inaccurate. Even if better paper were used, all the problems inherent in a paper ballot recount would be in place. These include questions about mutilated or hard-to-read ballots, the possible loss or manipulation of the paper ballots, and the fact that no two recounts yield the same result. In short, the voter verified paper trail does not provide a real safeguard and it has significant operational problems. The best safeguards are those discussed above – certification, testing and management systems for DREs, as well as all other voting systems.

MEMBER RESPONSE: If a voting machine has been programmed to print out an incorrect paper ballot ("a misleading confirmation"), then this will be detected by those voters who read and verify their ballots, thereby detecting that the vote has been incorrectly recorded. That's the whole idea!

The LWVUS is simply wrong when they argue that we cannot count paper accurately. Banks appear to have successfully counted paper money for years. Countries such as Canada and Switzerland use paper ballots and have reported no difficulties in counting them. Racetracks and lotteries deal very well with paper. Who has decided that the only area in which we can't deal with paper is elections?

Of course if the paper results were to differ with the results reported by the DREs, then we would have strong reason to suspect that the DREs are in error. After all, the voter has no way of knowing how his or her vote is recorded by the DRE, whereas with a VVPB the voter can read and verify that his or her vote is correctly recorded on the paper ballot.

QUESTION: Is the DRE a paperless system? Aren't there any records?

LWVUS ANSWER: Under the Help America Vote Act (HAVA) there must be a paper record of each vote from a DRE voting system. In well-run systems, the printouts with vote totals are taken throughout Election Day and compared to the total number of votes cast at the machine, to ensure security. The paper records then provide a backup for official tabulations of election results. In addition to vote totals, DREs can print out each individual ballot (without identifying the voter) to provide an additional security and audit capacity. Not only can this data be printed, it is saved electronically in multiple formats in multiple locations, so that if one mechanism fails the information is backed up using another format in another location. In other words, DREs in well-administered systems provide a substantial audit capacity for purposes of recounts and authentication.

MEMBER RESPONSE: The LWVUS leadership are aware of the fact that the paper records that are printed out at the end of the day are worthless as a form of audit or to conduct a recount. The appropriate word is "reread," rather than "recount," since all that these records do is to reflect the contents of the machine. If the contents of the machine have been corrupted, the paper records will also be corrupted.

The statement about printing out individual ballots is confusing. Does the LWVUS now advocate voter verified paper ballots? If not, of what use is the printing out of an individual ballot if the voter who cast that ballot cannot read the paper "record" and verify that it is correct? What does the LWVUS propose to do with the paper records?

The storage of data in multiple formats and multiple locations is a good form of redundancy (fault tolerance), but it provides no security if the data has been corrupted before it was stored in the first place. It could be of benefit if the initial data are correct, but the security problems derives from the possibility that the voter's vote could be modified before it is stored in the internal memory of the machine, in any location and in any format.

QUESTION: What are some of the other issues with a requirement for a voter verified paper trail?

LWVUS ANSWER: One important advantage of a DRE system is that it provides an opportunity for persons with disabilities and people with limited English capacity to vote privately and independently. The DRE is easily fitted with earphones for an aural ballot for persons with limited vision, including the elderly, and for persons with limited reading ability. For persons with physical disabilities, the computer interface system is easier to use than the optical scan system which requires the voter to successfully manipulate the marking pencil. For persons with limited English capacity, DREs can easily be programmed to accommodate multiple languages. A requirement for the voter to verify a paper ballot undermines access for citizens who have trouble seeing or who have limited English capacity, and can push election officials toward optical scan devices that are not as accessible for a broader range of citizens.

MEMBER RESPONSE: Is the LWVUS saying that we should not have voter verified paper ballots because people with vision and language problems may not be able to verify their own votes? Such a statement ignores the benefit that accrues to all voters if just some of them verify their ballots. Verification by sighted voters should detect problems with incorrect printing of the ballots.

According to an opinion issued Oct. 10, 2003 by the U.S. Department of Justice regarding HAVA

requirements as they relate to voter verifiable audit trails http://www.usdoj.gov/olc/2003opinions.htm:

> **"The ability to verify one's ballot before casting it is essential, cf. 15481(a)(1)(A)(i), but the availability of multiple techniques by which to do so is not. Disability accommodations often result in a greater range of methods by which non-disabled persons can accomplish their goals, yet such accommodations are not deemed to deny equal opportunities for disabled persons for that reason alone. Consider a building that provides both a set of stairs and a wheelchair ramp to its outdoor entrance. Non-disabled persons have more means to enter the building (they can use either the stairs or the ramp), while the wheelchair-bound person can use only the ramp. But no one would contend that such a building has deprived disabled persons of the 'same opportunity' to access the building. That is because the essential requirement of access -- the ability to get to the front door -- is available to all. The means to achieve that end differ, and non-disabled persons have a greater number of options, but provision of the ramp suffices to provide disabled persons with a similar (though not 'identical') opportunity. So too with the DRE voting systems, as you have described them."**

Furthermore, it is technically possible to have voter verified paper ballots that can be verified by people with vision problems. As discussed above, Vogue Election Systems (VES) has developed a machine that can be used by people with vision and language problems just as they would use a DRE. Instead of tabulating and counting the votes, the VES machine simply marks an optical scan ballot. That ballot can be read through an optical scanner with attached earphones and verified by the blind. It can also be verified by the sighted and counted, both by an optical scan machine and by hand.

There are other possible technical approaches for allowing people with visual impairments to verify their votes. For example, with Avante machines the signal for the printer is split off to the audio as a simultaneous feed. This means that the audio always matches the printout.

The bottom line is that it is possible to design and build computer-based voting machines that are secure and that provide the visually impaired voters with the ability to verify their votes. If this is not financially viable at this time, visually impaired voters still benefit from the ability of other voters to verify their votes.

QUESTION: Are there operational questions about the voter verified paper trail?

LWVUS ANSWER: Yes. Printers are among the least reliable of computer system components. They jam, they need paper, they are slow, and they are an added cost. Long lines are already a problem in many voting jurisdictions, and printing individual ballots for confirmation by each voter at the polling place will only exacerbate those problems, without adding to security. Voters' privacy is also at risk each time a printer jams and a poll worker has to work to remove the paper jam. Finally, the verification process in this format can be confusing to the voter and has not been fully tested in polling place operations.

MEMBER RESPONSE: Modern printers can be quite reliable and fast, and election officials can be taught how to install paper. In the rare case where the paper jams, the machine can be taken out of service until a new printer is installed.

This is not rocket science. We know how to build highly reliable printers. Admittedly, reliable printers are more expensive than unreliable ones. So we have to ask ourselves how much our

democracy is worth. The founders of the LWV, the women and men who suffered and went to jail in the fight for universal suffrage, thought it was worth a great deal. Prior to and during the Civil Rights Movement people died in the struggle for the right to vote. Does the LWVUS now argue that we cannot afford the additional cost of reliable printers to safeguard our votes?

QUESTION: Are there security and accuracy issues with the voter verified paper trail?

LWVUS ANSWER: Yes, there are significant security issues with a system that requires each voter to review, in private, an individual piece of paper. Each individual piece of paper in the voter verified paper trail system must be collected, protected, and prepared for a recount. As we saw in Florida in 2000, with nearly 6 million ballots cast in the Presidential election, this is a monumental task, with the possibility of lost, mangled and manipulated paper ballots. With these well-known problems with paper recounts, it is more likely that the paper recount would be in error than the electronically cast ballots from DREs with their required paper back-up records. In fact, when asked what would happen if there were a question about the accuracy of results with a voter verified paper trail system, one manufacturer of such devices, and an advocate for the VVPT, said that of course they would do a recount using the electronic systems. They would not even try to recount the individual paper confirmations.

MEMBER RESPONSE: One might equally well conclude from Florida 2000 that we should abolish paper currency, rather than paper ballots. Neither is a logical conclusion.

As we stated earlier, the voter is not required to review the voter verified paper ballot, though hopefully many voters would do so. This is an option, not a requirement. Of course the more voters who take the time to verify their ballots, the more confidence we will have in the reported outcome of the election.

Furthermore, the statement that it is more likely that a paper recount would be in error than that the electronically cast ballots from DREs would be in error is indefensible. The whole problem is that we have no way of knowing how often the DRE counts are in error, because we have no way to check or audit them. The LWVUS cannot possibly conclude that there would be more errors in a paper recount, since they have no way of knowing how many errors there are when the DREs record and tabulate votes.

While manual recounts that have not been carefully designed can be inaccurate, there are techniques for making paper counting efficient, precise, and accurate. It appears that many people running the recounts in Florida in 2000 were not familiar with these techniques. By contrast, California has had a mandatory 1% recount requirement for quite a while, and there have been no loud complaints about these counts being inaccurate, even when some voting districts in California were voting on punchcard machines.

Many countries, such as Switzerland, Canada, France, and the UK, have been counting paper ballots for years. Does the LWVUS believe that US citizens are less capable of counting than, say, Canadians?

Finally, it is very disheartening that the LWVUS takes the word of voting machine manufacturers while ignoring essentially the entire computer security community, as well as the more than 1700 technologists who have signed a petition calling for a voter-verified audit trail http://verifiedvoting.org/resolution.asp**.**

Surely the LWVUS does not feel that they need to serve as advocates for the manufacturers of DREs!

QUESTION: Is there an issue with certification of machines that can provide a voter verified paper trail?

LWVUS ANSWER: Approximately 40 states have chosen to follow the federal voluntary standards for certifying their voting systems. These standards are designed to ensure that voting machines meet basic reliability and security requirements. These standards and procedures do not currently provide for a voter verified paper trail. Developing standards takes a period of time to make sure that issues are properly addressed. The issues for the VVPT include what kinds of paper would be used, how it would interface with DRE machines, how the voter would verify or refuse to verify the paper record, how the individual paper confirmations would be handled and protected, and a host of other technical issues. Even if a VVPT requirement were advisable, there are serious practical and legal problems that must be resolved before moving ahead.

MEMBER RESPONSE: We agree that there should be sound standards and requirements for touch screen voting machines that produce a VVPT. However, the implication seems to be that no voting systems that provide VVPT have been certified. As noted above, certified optical scan voting machines by default produce voter verified paper ballots. Furthermore, the touch screen Avante Vote-Trakker received FEC/NASED certification on Nov. 6, 2002.

After thoroughly studying the issue, Kevin Shelley, the California Secretary of State, has determined that California will have to use voter verified paper audit trails starting in 2006.

Unfortunately, the money allocated by HAVA resulted in a rush to purchase inadequate and insecure DREs without first taking the time to determine how best to use computing technology to improve the security and reliability of our elections. We should immediately halt the purchase of paperless DREs and start developing proper standards and requirements for machines that provide a voter verified paper ballot.

QUESTION: Is there any protection to ensure my ballot says what I intend it to say?

LWVUS ANSWER: The new Help American Vote Act (HAVA) already requires that voting systems provide for "second chance" voting by 2006. While many had hoped for an earlier deadline, the practicalities of changing many voting systems quickly caused Congress to choose the 2006 deadline. Nonetheless, new machines being purchased now must meet the "second chance" voting requirement. That requirement means that before your ballot will be officially cast, you must have the opportunity to review it, change it, or request a new ballot. The voting system must also notify you of a possible "overvote" (such as voting for two candidates for President) so that you can make a correction. For DREs, this process occurs in the privacy of the polling place, the machine itself is programmed to make it difficult to make a mistake, and the system gives the opportunity to review the ballot before it is cast. With optical scan and punchcard ballots, the review function comes as the paper ballot is sent through a machine with the poll worker and other voters looking on. Finally, under HAVA, as described above, there must be a paper record of each vote from each voting system.

MEMBER RESPONSE: The short answer to the question is it depends on which voting system you

are using. There is absolutely no way to ensure that my ballot is accurately recorded and counted by a paperless DRE. By contrast, optical scan ballots are easily verified by the voter.

Furthermore, the anti-VVPB position of the LWVUS contradicts the HAVA requirement of a paper record of each vote. The claim made by the LWVUS that the print-outs made at the end of an election are paper records of each vote from each voting system is specious, since there is no way to know whether or not those print-outs accurately reflect the votes.

QUESTION: Haven't we always relied on paper. What about recounts?

LWVUS ANSWER: Much of the country has voted on lever machines for the past century. With lever machines, a recount consists merely of reading the machine again, without the benefit of an individual record of each vote cast, as DRE systems can provide. Human errors in reading the machines and counters that stick are real problems for lever machines. Paper ballots get recounted because of the inherent inaccuracies associated with the counting of paper ballots. When thousands of pieces of paper are counted, either by hand or by machine, mistakes are made, and so recounts are often needed if the margin of victory is small. Punchcards were a major advance over regular paper ballots because they are counted by machine. The problem, as we saw in Florida in 2000, is that the marking system (punching through the paper so the machine can count it) is sometimes incomplete (the "hanging" or "dimpled" chad). Similarly, optical scan systems sometimes have a marking problem, because the pencil used is not the correct one and so does not reflect the vote when the machine scans the paper ballot, or because the voter "incorrectly" marks the ballot with an X or incompletely marks the ballot. So recounts are necessary with paper ballots because of the inherent problems with paper ballots. Electronic machines do not have this problem. The accuracy of the counting is not really at issue. The issue with electronic systems, as discussed here, is whether the machine is accurately receiving the information from the voter. To guard against possible errors after the ballots are cast, new standards under HAVA require a paper record of each vote, as discussed above. From the recount angle, DREs are clearly better than paper-based systems. Brazil regained trust in the election process by replacing a fraud-ridden paper system with DREs in the late 1990s.

MEMBER RESPONSE: Electronic machines do indeed eliminate the possibility of a recount. If you think a mistake has been made, tough luck. Even if you have grounds to believe that fraud has been committed, there is no way to conduct a recount. The use of paperless DREs make it impossible either to prove or to disprove that the reported election results are correct, as the citizens of Broward County, Florida have learned. In a recent special election for the State House District 91 seat in Broward County, Ellen Bogdanoff won with only a twelve-vote margin out of 10,844 votes cast. Furthermore, there were 134 voters whose votes were not recorded, even though there was no other race on the ballot. Because the margin of victory was less than one quarter of a percent, Florida election law mandates a manual recount. But since the election was held on paperless ES&S DREs, there was no way to do a recount. And there was no way to determine the intent of the 134 voters whose votes were not recorded for any of the candidates.

Lever machines also eliminate meaningful recounts and are dangerously flawed. If anything, lever machines are an illustration of how easy it is for the public to develop a high degree of confidence in a deeply flawed technology that is subject to serious problems, including rigged elections.

QUESTION: I've heard that there is a question about election fraud in systems with paper receipts. What's that about?

LWVUS ANSWER: If the voter is given a receipt that shows how he or she voted, then vote-buying schemes can be very effective and voter intimidation can ensue. Because of the paper record, the vote buyer knows that the seller voted according to the wishes of the purchaser. If voters have a record of how they voted, then spouses, employers and others can ask voters to disclose how they voted or "pay a penalty." For these reasons, no system should allow a voter to take a voter verified ballot confirmation out of the polling place.

MEMBER RESPONSE: We agree that a voter should not be given a receipt. There is no receipt involved with a VVPB, since the paper itself is the ballot. If you walk out with your voter verified paper ballot, then you have essentially not voted.

QUESTION: If a voter verified paper trail makes people feel good, why not do it?

LWVUS ANSWER: The voter-verified paper trail adds costs and complications to the voting process, does not add significant security, and undermines disability and language access. To summarize: First, the voter verified paper trail is not necessary. Other mechanisms can provide necessary safeguards against security concerns. Second, the voter verified paper trail doesn't work. The individual paper records cannot be used accurately for a recount. Third, the voter verified paper trail requirement undermines access for persons with disabilities and limited English skills. Fourth, the voter verified paper trail doesn't add reliability to the system at the polling place. It complicates the polling process while the monitoring of machines during Election Day provides a similar safeguard. And fifth, the voter verified paper trail does not address the real election system problems that caused nearly six percent of votes to be lost in 2000, including registration database failures, ballot design problems and polling place operations. In short, VVPT can mislead the public into believing that the paper confirmation is a valid record of the vote.

MEMBER RESPONSE: This is not a debate about making "people feel good." It's a debate about whether or not we can have confidence that our votes are accurately recorded and counted. All of the LWVUS arguments contained in the above answer have been rebutted earlier. While it's true that a Voter Verified Paper Ballot does not address the issue of registration database failures, neither does a paperless DRE. We all agree that voter registration is an important issue, but it is irrelevant to this debate.

QUESTION: Our election system is so important. Shouldn't we insist that all voting systems have 100 percent accuracy?

LWVUS ANSWER: Yes, we should aspire to have perfection in our voting systems and continually work toward that goal. Technological advances over the years have vastly improved our voting systems. It would be difficult to imagine counting the millions of votes that are cast in a Presidential election without those improvements over the old hand-counted paper ballot. In their day, punchcards and lever machines were substantial improvements. But they have significant problems, such as "hanging chads" and mechanical errors. Marking, transporting, storing and counting paper ballots have been the sources of election irregularities in some areas. And so we are moving to better systems like DREs and precinct-count optical scan machines. Improvements will continue to be made even in these systems, particularly in the area of the "human interface," to ensure they are "user friendly."

MEMBER RESPONSE: Yes, we should insist on 100 percent accuracy as our goal. We

should use technology when it can increase accuracy, for example in eliminating over votes and stray marks on optical scan ballots. But, just as we do not trust technology that cannot be audited for activities ranging from banking to the lottery, we should not trust technology that cannot be audited for our elections.

QUESTION: What is the role of the new federal Election Assistance Commission (EAC) set up under HAVA?

LWVUS ANSWER: Once it is up and operating, the new federal EAC will have authority for the standard setting process for voting machines, in association with the National Institute of Standards and with the input of state election directors. The EAC will also develop best practices for election administration, examine emerging issues in election reform, and develop guidelines for the state certification process. The delay in nominating and confirming the four commissioners has delayed the EAC's work, which would include examination of potential security issues and deal with certification, testing and administrative practices to ensure voting machine security.

QUESTION: Why are voter education programs so important?

LWVUS ANSWER: When voters have had experience using their voting machines, there are many fewer errors in properly recording the voters' intent. Even a machine that does not work particularly well can have a low error rate if the voter is familiar with the machine, while even a good voting system can have problems if voters are seeing it for the first time. Thus voter education programs, that explain how to work the voting machines and give voters an opportunity to practice and gain hands-on experience before Election Day, are very important.

QUESTION: What about Internet voting?

LWVUS ANSWER: Voting over the Internet raises substantially more security issues because the voting machines and the official election site can be subject to penetration and manipulation. Many hope that on-line voting will be a part of future elections, but there are many issues that must be resolved before we can have confidence in such systems.

MEMBER RESPONSE: We agree. But the security risks with Internet voting that must be resolved are so fundamental that they are not likely be resolved in the near future. If they are ever resolved, it will be only by a total redesign of personal computers and the Internet itself.

QUESTION: I've heard that Miami replaced its voting machines after the 2000 election and still had problems in the 2002 election?

LWVUS ANSWER: Miami-Dade County replaced its punchcard voting machines with new DREs for the 2002 election. Because of inadequate poll worker training, many of the machines were not plugged in, turned on or warmed up before the primary election, and there was confusion at the polls. For the general election, county and other officials were brought in to work at the polls, and the election proceeded more smoothly. This indicates, once again, how important it is that there be an integrated approach to improving voting systems. Good machines are needed, but so too is poll worker training and good administration.

MEMBER RESPONSE: The LWVUS is correct in saying that Miami-Dade had problems in the primary elections because of inadequately trained poll workers. However, as was observed by the report of the Miami-Dade Inspector General on the Sept 10, 2002 primary http://www.miamidadeig.org/reports/voting%20final%20report.pdf**, there were also significant problems with the machines and the software. The Inspector General's report concluded that "[T]he debacle [of the September 10, 2002 primary] was, in large part, caused by the exorbitant set-up time required by the ES&S devices."**

The problem of the lengthy set-up time required by the ES&S DREs continued into the November, 2002 election. According to independent observers from the Center for Democracy http://www.centerfordemocracy.org/mia/MDFNLRPT.pdf**, the amount of time required for advanced preparation in Miami-Dade was extremely lengthy, primarily because the ES&S iVotronic devices each required 8 to 70 minutes to activate. Since the devices had to be activated separately and in sequence, the number of person-hours required countywide was enormous. While most poll workers and specialists had anticipated that the ADA machines would require 35 minutes to boot up and the regular machines 5 to 6 minutes, in fact the ADA machines required 65 to 70 minutes, and the regular devices 6 to 10 minutes.**

To avoid another election crisis because of extended boot-up time, the County powered up the voting machines the day before the election. The machines were guarded overnight by police, with a cost of about $2.1M for approximately 47,500 hours of police overtime.

While "county and other officials" helped make the November election more successful, as the LWVUS claims, this comment ignores the fact that the officials were needed to respond to problems with the machines and that the cost of their involvement was extraordinarily high. (The total additional cost for the November election was $3.8M).

Furthermore, according to the County Manager Post-Election Analysis http://www.reformcoalition.org/ressources/Post%20Election%20Analysis&Recommendations.pdf**, "Success rates for the use of these devices by the sight-impaired were not acceptable." "Numerous problems with audio units including lengthy opening and activation time, shutdowns, difficulty with navigation, and failure to read ballot exclusively in selected language."**

The Florida ACLU also studied the September 2002 Miami-Dade primary http://www.aclufl.org/news_events/archive/2002/racialimpactrelease.cfm**. According to the Miami-Dade Election Reform Commission: "A study of 31 problem precincts conducted by the Florida ACLU found that 18,752 voters signed the rolls to vote, but only 17,208 votes were recorded. This means that a total of 1,544 votes were lost in those precincts, a lost vote rate of 8.2%. The ACLU reported that approximately half of the lost votes were from African-Americans. These lost votes echoed the failures of the 2000 election. According to the Miami Herald, the rate of under- and over-votes in those 31 precincts had been 6.75% in November 2000. The ACLU also reported a large disparity when the rate of problems at majority black precincts was compared with the rate in majority non-black precincts."**

In other words, a higher percentage of African American votes were "lost" by the ES&S machines

than had been lost by the infamous punch card machines. There was no way to determine what the intention of those voters had been, because there were no paper ballots.

QUESTION: What are the most important problems in our election systems?

LWVUS ANSWER: The 2000 election exposed a large number of very serious problems in our election systems, from voting machines that don't work well to poor ballot designs, from erroneous purges to eligible voters being turned away from the polls because of poor administration of the voter rolls. According to an official report from the California Institute of Technology (Caltech) and the Massachusetts Institute of Technology (MIT), four to six million votes were lost in the 2000 Presidential election. Between 1.5 and two million were lost because of faulty voting equipment and confusing ballots, 1.5 to three million were lost because of voter registration mix ups, and up to one million were lost because of polling place operations. Congress responded by passing the Help America Vote Act (HAVA) which requires states to improve election administration and protect voting rights through new federal requirements, including provisional ballots, statewide computerized voter lists, "second chance" voting that helps to ensure the proper casting of ballots, and disability access. In addition, states were required to develop election reform implementation plans, which each of them has now done. Federal funding is being provided to implement the reforms described in state implementation plans.

QUESTION: What's the bottom line on DREs?

LWVUS ANSWER: DREs, like all voting systems, must be carefully designed and tested, and there must be rigorous security and management systems. DREs bring important advantages to the election system, including ease of use, and disability and language access, while precinct-count optical scan machines can be an option as well for states upgrading their voting machines.

MEMBER RESPONSE: Even if the manufacturers of the current crop of DREs were to employ rigorous security measures, we would still not know whether or not the results reported by the machines were an accurate reflection of the voters' intent because of the unavoidable risks of malicious or buggy software.

QUESTION: Where can I get more information?

LWVUS ANSWER: The League of Women Voters website, at http://www.lwv.org/join/elections/hava_resources.html has additional background information, including papers by recognized experts in the field.

MEMBER RESPONSE: The LWVUS refuses to print on its website any information that contradicts its position in support of paperless DREs or any responses from opponents of paperless DREs, no matter how well documented, even from League members and world renown scholars. See http://www.verifiedvoting.org for more information about the risks of DREs.

Questions the LWVUS Should Have Asked, but Didn't

QUESTION: Have there been any documented problems with elections using DREs?

MEMBER ANSWER: Yes! There have been serious failures in elections conducted on DRE systems in Florida, Mississippi, Maryland, Virginia and Connecticut involving lost ballots and transposed votes.

For example, when the polls opened in Hinds County, Mississippi in November 2003 the electronic voting machines were not working, and there were no back-up paper ballots. By mid-morning, some machines were still not working. Voters had to wait in long lines and to use paper ballots without adequate privacy protection. People were still standing in line at 8 PM. On January 21, 2004 the Mississippi Senate declared the results from the District 29 November election invalid and voted to rerun the election on Feb. 10, 2004 http://www.verifiedvoting.org/article.asp?id=997).

QUESTION: Have there been cases in which blind voters have had problems using DREs?

MEMBER ANSWER: Yes. While in principle DREs can be adapted to enable persons with visual disabilities to cast ballots independently and in private, doing so is not necessarily easy. For example, the Miami-Dade County Manager's Post Analysis Report & Recommendations, pages 10 and 21 http://www.reformcoalition.org/ressources/Post%20Election%20Analysis&Recommendations.pdf states that the audio menu was poor and the success rate was not acceptable for blind voters using the machines. The report recommended adding headsets & visible screens for assistants -- which would of course eliminate both privacy and independence. Miami-Dade currently has paperless DREs manufactured by ES&S.

Acknowledgments: I would like to thank David Bowen, Martha Mahoney, Doug Jones, Linda Freedman, Diane Park, Shirley Jin, Carol Watts, Ellen Theisen, Gen Katz, Ernest Dieterich, and the many colleagues – computer scientists and LWV members – who have helped me prepare this response.

Disclaimer: Although I am a member of the League of Women Voters, any views presented in this document, aside from the LWVUS Question-and-Answer pairs, are mine alone and are not intended in any way to represent the current opinion of the League of Women Voters.