STATEMENT BY KAY J. MAXWELL
PRESIDENT, LEAGUE OF WOMEN VOTERS OF THE UNITED STATES
FOR
THE ELECTION ASSISTANCE COMMISSION
ON
ELECTRONIC VOTING SYSTEMS

May 5, 2004

Thank you, Mr. Chairman, for the opportunity to present the views of the League of Women Voters on the controversy over electronic voting systems.

The League of Women Voters is a nonpartisan citizen organization that has worked for more than 80 years to educate the electorate, register voters and make government at all levels more accessible and responsive to citizens. We believe that voting is the most important expression of a citizen's participation in government.

OVERVIEW

Mr. Chairman, the immediate issue facing this Commission, and our Nation, is the 2004 general election. Our Nation cannot afford to have a replay of the 2000 general election, when voting systems failed to properly record voters' intent, when purging and other election practices undermined voter participation, and when millions of Americans questioned the outcome and legitimacy of the presidential election.

Mr. Chairman, the 2004 election is in danger. Reforms necessary to prevent a replay of the 2000 election have not been put in place. Most Americans will vote on the same voting systems or machines that they did in 2000. Actions to ensure proper and accurate voter registration rolls are not complete, and many jurisdictions have not even really begun to implement such reforms. Citizen concern about the security of voting systems, access to the vote, and the counting of votes threatens the legitimacy of the upcoming election.

The controversy over electronic voting is just one warning sign about deeply-held suspicions about our election systems. These concerns must be dealt with through real-world safeguards to protect the vote and to assure Americans that their votes will, in fact, be protected.

The League of Women Voters believes that effective steps must be taken immediately to protect the right to vote. We call on the Election Assistance Commission to promulgate emergency best practices for the 2004 election to protect election security and to ensure voter access.

General security measures – such as enforceable statewide security plans**;** physical protection of voting systems from tampering**;** standards to govern machine preparation, testing and vote counting**;** and polling place practices to ensure that machines work properly – must be put in place.

In addition, specific security measures for each significant type of voting machine must be implemented. Punch card machines, optical scan machines, electronic machines, lever machines, and other systems each can be better protected if the Commission sets out specific management practices aimed at ensuring security and safeguarding voter access.

We must remember that Americans will vote on a variety of machines in 2004. Any solution to voting security and access problems must deal with each of these systems, not just with any single system. In 2004, punch cards will be used by approximately 20 percent of the voting public. Lever machines will be used by about 15 percent. Optical scan systems will be used by approximately 30 percent. And electronic systems will be used by about 30 percent. These figures are based on data from Election Data Services (EDS). Each type of voting system raises particular security and access concerns that must be addressed before the 2004 election.

Let me provide some examples. To properly record votes, punch card machines must be cleaned out before Election Day, so that remaining chads do not interfere with the voter's attempts to punch through the card. Optical scan machines must be calibrated to ensure the machines properly count each voter's vote. And DRE machines must have the correct ballots properly loaded in the machines. Although these examples seem basic, in reality they are not always followed. These types of real-world concerns should be dealt with in emergency best practices by the Commission.

We understand that the powers of the Commission under the Help America Vote Act (HAVA) are limited. The EAC does not have the power to compel states and localities to take particular actions. At the same time, the leadership role of the Commission should not be underestimated. At this time of deep citizen concern, when election officials are working hard to maintain citizen trust, action by the Commission can point the way to the effective steps that must be taken to protect the 2004 election. The Commission, working with election directors, technical experts, and concerned organizations, can promote sound election practices by establishing emergency best practices for 2004.

In addition to best practices to ensure security and access, we believe the Commission should give attention to best practices for the provisional balloting process in the 2004 election. It is easy to imagine that the outcome of the 2004 presidential election will be determined in a swing state by the counting of provisional ballots. Yet if that state does not have uniform standards and procedures for providing, handling and counting provisional ballots established before the election, there could be significant problems, including problems that fall squarely within *Bush* v. *Gore*. We urge the EAC to provide guidance to the states on provisional balloting, including issues of transparency and uniformity. Citizens will want to know how many provisional ballots were issued and what the standards and processes will be for counting such ballots in a fair and uniform way.

States and localities also bear primary responsibility for developing and implementing the management and procedural protections that are needed to protect voting systems, ensure the proper counting of all ballots, including provisional ballots, and ensure equal access to the vote for all eligible Americans. The League of Women Voters is deeply concerned that this is not happening, or is not happening fast enough. This Nation must ensure a fair and accurate election in 2004 and reassure Americans that the election will be both fair and accurate.

At a time when election systems are in flux, when citizens are asking hard questions about election administration, and when the political system is evenly divided along partisan lines, the temptation to look to conspiracy theories or to point the finger of blame can be strong. We in the League support a different approach. As a responsible organization, but one deeply concerned about America's election system, the League supports a working partnership among election officials, concerned citizens and organizations, and the EAC to ensure that specific effective safeguards can be put in place for 2004 and beyond. Election reform needs were neglected for too long before 2000 and are still under funded. In this situation, we must all look for practical, problem-solving approaches.

While the League does have concerns about the 2004 election process, it is vitally important that the debate not scare voters away from the polls. There is a danger that telling people that their vote won't count will discourage voter participation. We must always encourage people to vote, while we work to improve voter access and to ensure that every vote will count.

VOTING SYSTEMS IN 2004

The League of Women Voters believes that Direct Recording Electronic (DRE) voting systems can be an important part of election reform efforts. DREs bring significant advantages to our election system, including improved access for persons with disabilities or limited English proficiency**;** voter verification of ballots, including "second chance" voting in private**;** safeguards against "overvoting**;**" consistent and accurate counting of votes**;** and paper records for authentication, recounts and audits.

At the same time, important questions have been raised about the security of DREs, and about the management and operational practices that affect DRE performance in the real world. We in the League of Women Voters take these questions very seriously, and we believe they must be dealt with by this Commission, state and local election administrators, concerned organizations like the League and by citizens across the country.

In taking these questions seriously, it is important to carefully examine each issue, and to craft solutions that meet specific problems. Too often in this debate, a panacea or a “silver bullet” has been suggested. Unfortunately, there is no “silver bullet” for the problems we face. We must do the hard work of matching problems to solutions in a rigorous way.

Voting machines are instruments within a complex election system. The key is to design an overall system that builds in multiple checks making it improbable that the system will be tampered with and that ensures that the voter’s intent is properly recorded. Like any other tool, a DRE that is not properly tested, maintained, managed and operated will have substantial problems. Thus it is vitally important to take steps to ensure that DRE systems, as well as other systems, are properly managed.

Like DREs, precinct-count optical scan voting systems are compliant with the Help American Vote Act (HAVA), provided they are supplemented with a DRE at each polling place to provide for private and independent voting for persons with disabilities. Some prefer this type of mixed system**;** others believe that all-DRE systems are better.

In any case, it is vital to ensure the certification, testing, and accuracy of the soft- and hardware used in voting systems. We should not assume that only one type of voting machine is vulnerable to attack, mismanagement or operational problems. We are concerned that issues about the accuracy and reliability of DREs may apply to optical scan systems as well, and we know there are significant problems with the other types of systems that are not HAVA-compliant.

Because the 2004 general election is just months away, it makes sense to focus on the problems and possible solutions we face immediately. It may be that more systemic solutions will be needed. But now – six months before a presidential election – is not the time to make major nationwide changes in our election systems. Murphy’s Law has not been repealed, and our election system is large and diverse. Now is the time to make management and operational changes that are needed and that can be absorbed before November 2004.

As we examine voting systems, including electronic voting systems, in the 2004 context, there are several important principles that should be kept in mind:

First, security, reliability and access are important. These three items are the touchstones for effective voting systems. Currently, we lose too many votes in this country. When evaluating existing voting systems, and in thinking about new systems for the future, it is essential that we compare the problems of residual votes, voter access and system security among all types of voting systems. The residual voting rate represents the votes that do not properly record the voter’s intent, or don’t record any vote at all because of problems in voting mechanisms. This is an ongoing problem that regularly means that millions of votes are lost.

Second, fix the things that are broken. It is important to fix the problems in places where DREs, or other systems, are not working properly. We believe that emergency best practices related to operational and management issues can deal with these problems, but if particular machines, or sub-types of machines, or machines by a particular manufacturer are the problem, then those machines should not be used. We must be able to protect our voting systems.

What should be done to improve DRE reliability and security in time for the 2004 election? Actually, quite a bit. Among these are:

- physical isolation of each machine to protect against "hacking;"
- thorough review and testing during certification;
- maintaining election official control over ballot creation, loading ballots, source codes, and management systems**;**
- statewide security programs binding on jurisdictions**;**
- improved equipment management practices and polling place operations**;**
- testing prior to and after Election Day**;**
- and parallel monitoring during Election Day.

Third, voter confidence is important – for all voting systems and in all states. It is misleading to act as if there is only one kind of voting or voting technology problem when American voters will use many different systems in 2004. More than two-thirds of voters will vote on systems other than electronic machines, and many voters may still have reason to doubt – as they did in 2000 – that their vote will count. Polling data indicates a high degree of public acceptance of electronic voting systems. Electronic voting systems rate higher than other competing systems, including optical scan systems. This information is from InfoSentry Services using data gathered by Opinion Research Corporation. Voters in Georgia, who used statewide DREs for the first time in 2002, have a very high satisfaction rate, according to research by the Carl Vinson Institute of Government. At the same time, some jurisdictions have had problems with DREs, and this cannot help but undermine voter confidence.

Fourth, DREs, like all voting systems, don't exist in a vacuum. Voting systems must be carefully designed and tested, and there must be rigorous security and management systems. As was just alluded to, there may be machines in place that just won't work properly. But that should not be a condemnation of all electronic voting machines or all optical scan machines. Most problems we have seen can be dealt with through management and operational practices, especially including procedural standards, and poll worker and voter education.

Fifth, use of state-certified systems that meet federal guidelines and standards is a fundamental safeguard. There have been reports of the use of uncertified systems. This is simply unacceptable. Certification standards serve a number of vital functions. Federal standards protect voters through such requirements as the new "second chance voting" provision. Federal guidelines and state certification deal with such issues as reliability, audit techniques, and security standards that are basic to ensuring that voters' ballots will be properly cast and counted. Certification also assists state and local governments in the selection and implementation of voting systems by providing technical specifications, testing and reliability measures, and operational standards, and helps ensure that they are not excessively reliant upon voting machine manufacturers. National standards exist to ensure that a vote in California is just as likely to be counted as a vote in Virginia, and they cover an extremely wide range of physical and administrative issues. Bypassing certification, using uncertified systems or using systems for which guidelines and standards haven't been set is asking for trouble. Basic accuracy, security and access goals must be met, not avoided.

Sixth, voting systems must not result in discrimination. Older voting machines have repeatedly been shown to have varying rates of error depending on the characteristics of voters, including socioeconomic status and education level. Persons with disabilities have historically been forced to vote separately, but never equally, with voting systems that don't allow them to cast a secret ballot or to vote independently. Persons with limited English proficiency have also been prevented from having equal access to voting by machines and balloting systems that don't recognize their needs. Only electronic voting systems are currently able to provide full equality to people with disabilities or limited English proficiency. In addition, DREs have lower error rates for historically disenfranchised populations.

Seventh, voter verification or "second-chance voting" is important. HAVA requires for the first time that a voter must be able to review his or her ballot before it is officially cast and counted, and must be given the opportunity to change the ballot or receive a new one. This is the requirement for voter verification. DREs meet the voter verification provision by requiring the voter to review the ballot prior to officially casting his or her vote via a final review screen. DREs also easily allow the voter to make changes to the ballot before it is cast, and this is done within the secrecy of the voting booth. Optical-scan and other paper-based systems require the issuance of new ballots if the voter wishes to make a change, and often the review process is not carried out privately, undermining the secrecy of the ballot.

Eighth, technology is developing. We probably don't have all the answers today that we will need to improve the election system for 2006 and 2008. It may well be that the voting system or systems our Nation should be using have not yet been designed. Access issues, particularly related to the human interface with voting machines, need to be addressed for DREs and other systems in order to reduce residual voting rates, or "lost votes." Security issues, and security solutions, also are still developing.

ADVANTAGES OF ELECTRONIC VOTING SYSTEMS

DREs make it possible, for the first time, for persons with visual disabilities or limited manual dexterity to cast secret and independent ballots. This is accomplished through the use of earphones and other adaptive devices. Because DREs can be programmed in multiple languages, voters with limited English proficiency can also participate fully and equally. In addition, the millions of Americans who face literacy challenges can take advantage of the audio features of DREs to cast independent votes without embarrassment.

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. DREs also reduce many of the operational problems in handling paper ballots that have sometimes led to significant election irregularities. Election history is replete with cases of fraud committed through the simple expedient of manipulating, altering or losing paper ballots.

Well-managed DRE systems such as that in Georgia have strong public support, improve access and reduce errors in the casting and counting of the vote.

As their name indicates, Direct Recording Electronic voting machines directly record votes. Thus they provide accurate counts. According to federal guidelines, there must be a paper record of each vote cast for the purpose of audits and recounts**;** DREs can also provide paper records of each ballot for audit and authentication purposes, while preserving the anonymity of the voting process.

SAFEGUARDS FOR DRES

Many of the problems with DREs that we hear of in the public discourse are not really security problems, but operational and management problems. If voting machines don’t start up properly, or if poll workers have not been trained sufficiently in their operation, it is not really a security issue, and a paper trail will not address those problems. If there is a problem with batteries being discharged so that machines are not ready to operate, as apparently was a problem recently in California, that’s a management issue, not a security problem. We believe that it is important to distinguish the particular problems that must be addressed, so that they can be addressed specifically, rather than with a catch-all solution that won’t address specific problems.

We believe there are two fundamental issues facing DREs. First, are DREs safe? Second, what should be done to improve DRE reliability and security? The same degree of analytical rigor must be directed at each question.

Are DREs safe? There is reason to be concerned. There are significant examples of DREs being mismanaged. This mismanagement must be addressed before the 2004 general election by the appropriate authorities. DREs in well-run election systems are safe, at least on a relative basis with other voting systems, and have substantial advantages over other systems, as discussed above. 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. 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.

However, there are clear examples of DREs being used in ways that are not well-managed. Installing uncertified systems, allowing access for technicians without proper oversight, failing to properly test or prepare voting machines for Election Day, or skimping on poll worker training can each lead to significant problems.

What should be done to improve DRE reliability and security? As mentioned above, there are a number of steps that must be taken for the 2004 election. Among these are: physical isolation of each machine to protect against "hacking;" thorough review and testing during certification; use of certified systems only; maintaining election official control over ballot creation, loading ballots, source codes, and management systems**;** statewide security programs binding on jurisdictions**;** improved equipment management practices and polling place operations**;** testing prior to and after Election Day**;** and parallel monitoring during Election Day.

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 to 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.

Certification and testing is also important. Voting machines should be scrutinized by state officials and computer specialists before a machine is certified for use in their states. Voting machines also should be tested to guard against malfunctions, and management systems should 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 national standards and guidelines in most states. Second, voting systems must comply with state certification standards. Third, the individual machines are tested when they are delivered by the manufacturer to election officials. Fourth, the machines are tested just before Election Day. Fifth, 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.

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. 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. Computer specialists also point to testing and monitoring on Election Day as an additional safeguard. 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.

There is considerable public confusion about paper records and recounts. Under 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.

New DREs also provide for “second chance voting,” as previously mentioned. This 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 voter the opportunity to review the ballot before it is cast. With optical scan and punch card ballots, the review function comes as the paper ballot is sent through a machine with the poll worker and other voters looking on.

VOTER-VERIFIED PAPER TRAIL

Some who have raised concerns about DREs propose a particular solution – the so-called voter-verified paper trail (VVPT). We urge the Commission to look very closely and carefully at this proposal. As a solution to election problems, it deserves and requires as close and as critical an examination as is applied to DREs and to other voting systems in the first place. It makes little sense to criticize DREs, and then propose a solution that may leave the election system less secure or less accurate, or that may raise more questions than the problems it is meant to solve.

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 for the voter to look at if she or he wishes, and systems that would require that each voter actually verify the paper record of his or her vote.

Let us be clear that the VVPT system does not solve the operational and management problems we have seen with improper start ups, rundown batteries, or poor polling place operations. While one might think from reading some of the press reports that VVPT is a universal problem solver, it obviously doesn't solve problems if the machines aren't up and running properly in the first place.

We believe there are a variety of questions that should be answered before we go down the VVPT route. In examining these types of questions, the League has not been persuaded of the wisdom of VVPT systems.

First, does the VVPT really add security, and if so, how?

Second, does every voter have to verify his or her ballot, or is there value to unverified paper records?

Third, what does it mean to be voter verified? Will the paper record be as legible and accessible as the voting machine itself? How will the process of voter verification, whether it is required or optional, be carried out at the polling place?

Fourth, what happens if a voter says the paper record is incorrect? In other words, what is the process if the voter affirmatively does NOT verify? In this case, how is the electronic record or the paper record, or both, corrected and the ballots accurately counted? What if a voter is simply confused?

Fifth, how will the paper records be counted or recounted? What are the standards of accuracy that must apply to the counting of the paper records? What mechanisms for protecting the paper records will be put in place to guard against manipulation or loss?

Sixth, what is the official record of the vote? Will the electronic tally count under the VVPT system, and if so, when and under what conditions? When will the paper records be relied on? What are the effects of an ambiguous outcome?

Seventh, how will the system work mechanically? What certification and other standards will apply to the printers, the paper records, the counting devices and the security systems for the paper records?

Eighth, what is the affect of the VVPT system on voting access for persons with visual and physical disabilities, persons of limited English proficiency and persons of limited literacy? What are the associated socioeconomic impacts?

Let us look at the two different types of VVPT systems: Under the first system, the voter actually verifies each vote**;** under the second system, the voter has the option to verify his or her vote, but there is no assurance that any voter verified any particular paper record.

Proponents for the VVPT make the case that it provides back-up security in the case of malfunctioning DREs. They argue that the paper record can be counted to accurately determine the outcome of an election if DREs fail.

For the VVPT system to work as a backup for counting the vote accurately, it seems that every voter must verify every ballot. Otherwise there is no assurance that the paper trail is accurate. Unverified pieces of paper don't add accuracy or security. They may, or may not, reflect the voter's intent.

If there is a system for every voter to verify every paper record, then the paper record can, in theory, work as a counting mechanism. But this is a very tall order. Setting up reliable means for voters to verify, or, more importantly, refuse to verify, their ballots at the polling place adds a significant burden at the polling place. What happens if the voter chooses not to verify the record? What happens to the rejected paper ballot? Is the electronic record going to be corrected? If so, how? If only the paper record is corrected when the voter affirmatively rejects the first paper record, then the DRE mechanism itself is superfluous. In effect, the costly internal mechanisms of the DRE would be disregarded and the DRE system would be reduced to being a paper-record generating device.

Even with paper records that are actually voter verified, there are significant remaining questions. There are questions about the accuracy, reliability and fraud-potential for the counting of paper records, with the long history of lost, mangled and manipulated paper ballots. There are also questions about the technical specifications regarding the paper records – their legibility for the voter, their readability for the counting devices, and the specifications and reliability of the printers. These questions must be rigorously analyzed, and the results and risks must be compared to other systems.

Each individual piece of paper in this 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, is it more likely that the paper recount would be in error than the electronically cast ballots from DREs?

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. 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.

The paper printed out from add-on printers for DREs can use script paper, like that in an ATM, or thermofax paper, like that in a fax machine. Counting such paper accurately is a problem. Even if better paper were used, all the problems inherent in a paper ballot recount would be in place, including the likelihood that no two paper recounts yield the same result.

Now let's look at the VVPT system where there is no requirement for voters to verify their ballots. Some proponents suggest that the VVPT is an option for the voter. Does this provide security or reliability? If so, how?

It is unclear why we should rely on unverified paper records for a recount or for determining the outcome of an election. If the voter does not verify the record, how can we know it is reliable?

An alternative theory of the VVPT holds that the paper record is valuable even if voters aren't required to verify it. It is suggested that the VVPT would indicate that a particular machine is malfunctioning. In this example, the voter checks the record, discovers it is incorrect, and calls this to the attention of the poll worker. The poll worker pulls the machine off line for checking and repair. Under this scenario, the VVPT operates as an early warning system for the DRE machine.

But there are a number of problems with this example. First, if a malicious programmer or an outside "hacker" can change the electronic record of the vote, certainly such a skilled person can make the printer provide a paper record that doesn't expose any error. In other words, if I vote for candidate A, but the malicious programmer makes it so the electronic record says candidate B, the programmer could also make the paper record for candidate A. Under this scenario, the voter and the poll worker are not alerted to the problem. So, in this example, the paper record does not indicate a problem with the machine, and does not provide a safeguard.

Second, what happens if nine voters choose not to look at their paper record, but the tenth voter reports that her or his paper record is wrong? Should we assume that the previous nine votes were also wrong? Do we need to call those voters back and ask them? Do we need to somehow retrieve their votes from the system? Under the optional verification system, we clearly cannot rely on those unverified pieces of paper for a later recount.

There is also an issue with certification of machines that can provide a voter-verified paper trail. Federal guidelines and state certification 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 in a safe, secure and reliable manner with DRE machines**;**
- how the voter would verify or refuse to verify the paper record**;**
- what is the legibility of the paper record**;**

- how the individual paper confirmations would be handled, protected and counted**;**
- printer specifications and reliability**;**
- and a host of other technical issues.

As we understand it, some VVPT systems may have been "certified," but we are not aware that they have been certified according to the types of guidelines and concerns outlined above that deal specifically with the key issues and concerns.

Finally, we are concerned that the VVPT system can reduce access for persons with disabilities, limited English proficiency and low literacy. The VVPT system provides for the voter to verify the paper ballot, which historically disenfranchised voters will find difficult to do if they cannot see or if they have difficulty reading the paper verification. Private and independent voting is important, and, at this juncture, seems inconsistent with the VVPT system for significant numbers of voters.

These are questions and potential problems with the VVPT system. We believe they are sufficiently severe that the VVPT system, of either the optional verification or mandatory verification model, doesn't make sense for 2004. We are concerned that it doesn't make sense for the long term either, but technology is constantly changing and the debate over election systems is still developing. We are open to possibilities. We are looking for improvements in electronic security generally, reductions in the residual vote for all types of voting systems, and better human interfaces for electronic voting systems.

Mr. Chairman, the League of Women Voters believes our Nation must focus on solving the very real operational and management issues for voting systems in 2004. We urge the Election Assistance Commission to assist states and localities in this task, and we pledge our assistance in those efforts.

Thank you.