THE LEAGUE OF WOMEN VOTERS®
OF THE UNITED STATES

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

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

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.

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

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.

QUESTION: Then why is there such a debate?

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.

1730 M STREET, NW, SUITE 1000, WASHINGTON, DC 20036-4508
202-429-1965 FAX 202-429-0854
Internet: http://www.lwv.org E-mail: lwv@lwv.org

QUESTION: What are DREs?

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.

QUESTION: What are the advantages of DRE systems?

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.

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

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?

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.

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

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.

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?

ANSWER: Voting machines <u>can</u> 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.

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

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.

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

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).

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?

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.

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

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.

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

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.

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?

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.

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

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.

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

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.

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

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.

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

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.

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

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.

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

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.

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

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.

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

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.

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

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.

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

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."

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

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?

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?

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.

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

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.

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

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?

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.

QUESTION: Where can I get more information?

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.