PURPOSE – **The League of Women Voters Monterey Peninsula (LWVMP), California, recommends the following two approaches to strengthen the League's position on elections.**

I. Policy Review - Review the existing LWVUS policy position titled "Voting Rights: Citizen's Right to Vote. Protect the right of all citizens to vote; encourage all citizens to vote."
Recommendation: **to add the promotion of integrity and transparency in voting systems.**

SCOPE: The widespread use of electronic voting systems has led to many problems. These machines have an extensive history of errors, malfunctions, inaccuracies and are susceptible to hacking and fraud. Electronic voting systems force all tabulations to be performed in secret, under proprietary rules of vendors. This lack of transparency begs for review. If voters do not have confidence in election results, how can we expect their participation? The "right to vote" is reduced to a sham if the perception is that the result cannot be trusted.

Numerous government and university studies have shown the inadequacies of electronic voting systems. But the LWVUS has only addressed these issues via non-binding resolutions at Conventions. Since its beginning, the League has stood proudly and solidly in favor of open government, transparency in its procedures, and public access to records and data.

The voting system parameters that should be addressed include:
1. Transparency, security, accuracy and recountability in voting systems
2. Auditable ballots (durable, privacy protected, original, voter marked paper ballots)
3. Requirements for timely, statistically valid, random audits of all elections
4. Promotion of citizen access and oversight of election procedures.

II. Adopt 2009 LWV California Resolution at 2010 LWVUS Convention, which stated that Transparency be added to the existing SARA Resolution.

RESOLUTION:
1.   Whereas, the League of Women Voters has been an active champion of openness and transparency in government throughout our history, and

2.   Whereas, problems arising from the use of electronic voting systems led to the LWVUS adoption of the SARA Resolution that our voting systems be Secure, Accurate, Recountable and Accessible, and

3.   Whereas, the principle of Transparency will improve the current SARA Resolution and enhance public confidence in elections, which are the basis of our democracy, and

4.   Whereas, election transparency means full public access to all election procedures in order to allow meaningful verification of ballot handling, tabulating, auditing and related election records, and

5.   Whereas, furthermore in January 2009, the LWVUS Election Audit Task Force issued its Report on Election Auditing which repeatedly emphasized the critical need for transparency; therefore be it

Resolved that the LWVUS add the principle of Transparency to the SARA Resolution.
Adopted by the LWVC Biennial Convention on May 17, 2009

RATIONALE
(Documents and sources included)

In the last few years, as electronic voting systems (methods used for casting and counting of ballots) have become common, so have malfunctions, false counts and other irregularities. In addition, security vulnerabilities exist from both outsider and insider manipulation. There is a large body of evidence documenting the failures of electronic voting. As a result, public confidence in the integrity of our elections has fallen.

Electronic voting systems are inherently not transparent. Important election data and procedural records produced by software cannot be publicly verified since they are within proprietary software unavailable to the public. Various convoluted procedures, machine-produced paper trails, and audit protocols have been instituted to attempt to compensate for the secrecy, but the secrecy still remains.

Without a vigorous commitment to the principle of transparency and the practice of public verification, a basic tenet of our democracy is absent.   Election integrity should not be solely dependent on technical specialist, government official or vendor verification. Election integrity should be grounded in transparency of the entire voting system.

Our elections must have full integrity. Election procedures must be designed such that outcomes can be both TRUSTED and VERIFIED. Election transparency means full public access to the totality of all election procedures in order to allow meaningful verification of ballot handling, tabulating, auditing and related election records

What Interferes with Public Confidence

Electronic voting systems have a history of errors, glitches, malfunctions, inaccuracies and failures and have not proven to be secure from hacking, fraud or corruption.

All electronic voting systems are controlled by corporate vendors, and are certified by private laboratories under the authority of U.S. Elections Assistance Commission. However there are problems. Vendors sell uncertified equipment. One testing lab was decertified for undocumented testing procedures. A recent study found another lab's accuracy test unable to measure machine accuracy or error rates.

Machine produced paper trails are not ballots, are not original and valid voting records, and therefore cannot be verified for accuracy. They are nothing more than a report produced by an internal, private and unverifiable computer source. Recounts of touch screen DRE tabulations are meaningless, since there are no original voter-marked ballots to review for voter intent or count accuracy.

Audits are a check on accuracy and are expected to inspire confidence. However, the California requirement for a 1% manual tally audit is not statistically relevant since some ballots can be excluded (mail-in and provisional ballots not processed by election night).   In the Humboldt County November 2008 presidential election, the required audit failed to reveal the loss of 197 votes from the final tally.

One issue seldom addressed is the tremendous potential for corruption and fraud in the manipulation of secret and proprietary electronic voting systems. There are enormous sums of money used by special interests to influence the outcome of some elections (both candidates and ballot measures). Money and power are huge inducements to corruption and fraud. Secrecy invites crime.

RECENT IMPORTANT ELECTION INTEGRITY REPORTS

CA Secretary of State: Report of Post Election Audits (7/07)

 "None of the pre-scored punch card and lever systems in use in 1965 are still in use today. They have been replaced by an array of complex, computerized systems… There has also been an enormous increase in the number of votes cast by mail. The complexity of these systems means there are many more ways in which voting systems can fail to capture votes correctly, lose votes, miscount votes, and be manipulated to yield incorrect results." (pgs 4-5). The post-election audit is *transparent* if the public can observe all parts of the process, see that the audit was properly conducted, and see that the outcomes of the races are correct. Transparency in the auditing process is crucial for public confidence. Pg 24
http://www.sos.ca.gov/elections/peas/final_peaswg_report.pdf

CA Secretary of State--Top to Bottom Review (8/07)

The California Secretary of State (SOS) led the nation in a top-to-bottom review (TTBR) of all electronic voting systems by teams of computer specialists. The August 2007 report documented security vulnerabilities and accuracy failures, most dominantly with DRE touch screen systems. As a result, the SOS decertified three electronic voting systems in California, including optical scan systems.
http://www.sos.ca.gov/elections/elections_vsr.htm

LWVUS Report on Election Auditing (1/09):

It promoted transparency as follows: "Verify that public, bipartisan or third-party monitoring of sensitive election procedures has occurred." and "All sensitive procedures should be open to monitoring..." and "the process of counting any ballot received and comparing should be done publicly..." and "...post-election audits should be independent of officials who conducted the elections." (Pgs 5, 16, 18) It promoted verifications and audits as follows: "Strengthening requirements for reviews of election procedures, testing voting equipment and auditing vote results can go a long way to restoring confidence in the fairness of the voting process and accuracy of election results." (p 3) and "   (T)he audit should be completed prior to declaration of the final official results." (p 14) and "Statistical principles must play a key role in (audits)…" (p 22).
www.lwv.org/Content/ContentGroups/Membership/ProjectsTaskforces/Report_ElectionAudits.pdf

Ohio Secretary of State Study: Voting Systems Vulnerable (12/07) "The Evaluation & Validation of Election-Related Equipment, Standards & Testing report, known as EVEREST, is a comprehensive review of voting systems revealing startling findings on voting machines and systems used in Ohio and throughout the country. Ohio's electronic voting systems have "critical security failures" which could impact the integrity of elections in the Buckeye State, according to a review of the systems commissioned by Secretary of State Jennifer Brunner."
http://www.sos.state.oh.us/sos/text.aspx?page=4512

2004 & 2006 LWVUS SARA RESOLUTIONS ARE INADEQUATE WITHOUT TRANSPARENCY

SECURITY is compromised when secrecy surrounds the internal processing of votes and ballot tabulations. The security of the vote and voting systems cannot be assured without transparency and public verification.

ACCURACY cannot be assumed if the counting process is performed unobserved and outside of public scrutiny and verification.

RECOUNTABILITY has traditionally depended upon voter marked ballots. Machine generated paper trail systems are not voter marked ballots. There is no assurance that these systems accurately reproduce or tally the vote that was cast. Without voter marked ballots, verification is not assured.

ACCESSIBILITY is required by the Help America Vote Act, but HAVA does not require the use of direct recording electronic (DRE) systems to support voters with disabilities. Other acceptable alternative (ballot-marking) devices are available.

RELEVANT DOCUMENTS, SOURCES AND QUOTES

1. Are Your Votes *Really* Counted? Testing the Security of Real-world Electronic Voting Systems (2008). "All voting systems recently analyzed by independent security testers have been found to contain fatal security flaws that could compromise the confidentiality, integrity, and availability of the voting process. Our experience suggests that there is a need for a drastic change in the way in which electronic systems are designed, developed, and tested. Unless electronic voting systems are held up to standards that are commensurate with the criticality of the tasks they have to perform, the very core of our democracy is in danger."   http://www.cs.ucsb.edu/~seclab/projects/voting/

2. Brennan Center: Post Election Audits: Restoring Trust in Elections (2007). The widespread adoption of voter-verifiable paper records does not, however, resolve the security, reliability, and verifiability issues with electronic voting that many groups, including the Brennan Center, have identified. To the contrary, …voter-verifiable paper records by themselves are "of questionable security value." Paper records will not prevent programming errors, software bugs or the introduction of malicious software into voting systems. If paper is to have any real security value, it must be used to check, or "audit," the voting system's electronic records. (p 8)
http://electionaudits.org/files/Brennan%20Center%20Report%20on%20Post-Election%20Audits.pdf

3. Center for Democracy and Election Management, American University (2007). The Carter-Baker Commission on Federal Election Reform Progress Report notes "... national failure of election laws and practices to allow independent observers to be present during crucial parts of the process." ...."This limits transparency and public confidence in the election process. Above all, elections take place for the American people, rather than for candidates and political parties. Interested citizens, including those not affiliated with any candidate or party, should be able to observe the entire election process."
http://www1.american.edu/ia/cdem/usp/np/cbc_progress_2007_06_12.pdf

4. CIA Expert says most electronic voting isn't secure (3/24/09).
http://www.mcclatchydc.com/227/story/64711.html

5. Computer Scientists take over Electronic Voting Machine with New Programming Technique (2009). Computer scientists demonstrated that criminals could hack an electronic voting machine and steal votes using a malicious programming approach that had not been invented when the voting machine was designed. By using just the information that would be available to anyone who bought or stole a voting machine, the researchers addressed a common criticism made against voting security researchers: that they enjoy unrealistic access to the systems they study.
  http://www.jacobsschool.ucsd.edu/news/news_releases/release.sfe?id=873

6. CRS Report to Congress: Election Reform and Electronic (DREs); Analysis of Security Issues (11/03). Library of Congress, Congressional Research Service. "While there are some differences of opinion among experts about the extent and seriousness of those security concerns, there appears to be an emerging consensus that in general, current DREs do not adhere sufficiently to currently accepted security

principles for computer systems, especially given the central importance of voting systems to the functioning of democratic government."(Pg 2) http://epic.org/privacy/voting/crsreport.pdf

7. Diebold admits audit logs in ALL versions of their software fail to record Ballot Deletions (2009)
The Humboldt County Election Transparency Project, using the free and open source software program Ballot Browser, found that Diebold's GEMS system had eliminated all votes from 197 vote-by-mail ballots cast during last November's general election. This approach- independently scanning ballots with separately developed open source software and off-the-shelf hardware - demonstrates the need for 100% audits. http://www.bradblog.com/?p=6995

8. Election Problem Log, 2004 to Date: Log of news reports about election problems.
http://www.VotersUnite.org/

9. Federal Certification Test for Count Accuracy Cannot Determine Error Rate (3/21/09)
"The test, which was designed by a federally-accredited test lab for the sole purpose of testing the accuracy of the vote-counting equipment, cannot prove whether or not the system accurately counts votes, nor can the test yield any measure of the accuracy rate. Such testing provides false assurance that a federally-certified vote-counting machine meets the accuracy requirements of federal law."
www.votersunite.org/

10. GAO Report: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed (9/05) This report concludes that electronic voting systems are deficient in security and reliability, and confirms that many irregularities in the 2004 presidential election could have affected its outcome. www.gao.gov/new.items/d05956.pdf

11. Humboldt (CA) Transparency Project (3/09) Hundreds of Lost Ballots and Illegal Voting System Illustrated by Simple Citizen Oversight, Free Open-Source Voting System in One California County...
http://www.pewcenteronthestates.org/uploadedFiles/wwwpewcenteronthestatesorg/Reports/Electionline_Reports/electionlineWeekly03.05.09.pdf

12. KY: Several Clay County Officials Arrested On Federal Charges (3/19/09). County election officials, including the circuit court judge, the county clerk, and election officers, were arrested on charges of conspiracy, the defendants were also indicted for extortion, mail fraud, obstruction of justice, conspiracy to injure voters' rights and conspiracy to commit voter fraud, including changing votes at the voting machine and showing others how to do it.
http://www.kentucky.com/210/story/731826.html

13. "Missing Pieces" - A Citizens' Review of the November 2008 Presidential Election in Riverside County, California (4/09) Save R Vote Report documents violations of election law and egregious failures by the Riverside County Registrar of Voters. She failed to conduct a 100% manual tally of all votes cast on the touch screen machines prior to certification of the November 2008 election.
http://www.electiondefensealliance.org/Riverside_Missing_Pieces%20

14. Ohio official sues e-voting vendor for lost votes (8/08) E-voting machines from Premier Election Solutions, formerly known as Diebold dropped hundreds of votes in 11 Ohio counties during the primary election. http://www.computerworld.com/action/article.do?command=viewArticleBasic& articleId =9112041&source=rss_topic17

15. Policy Mechanisms for Increasing Transparency in Electronic Voting (Fall 2008)
http://josephhall.org/papers/jhall-phd.pdf

16. Principles and Best Practices for Post-Election Audits (9/2008). This report has been endorsed by statewide election integrity groups in 12 states, also Common Cause, American Statistical Association and more. "Well-designed and properly performed post-election audits can significantly mitigate the threat of error, and should be considered integral to any vote counting system." Page 5.
http://www.electionaudits.org/principles

17. State (MD) Files Claim Against Premier, formerly Diebold (12/08) "Company Should Repay Money Spent to Fix Machines", Maryland Attorney General Says. The claim against Texas-based Premier, formerly Diebold, alleges that state elections officials were forced to spend $8.5 million to address a host of security flaws in the machines from 2003 through the November election.
http://www.oag.state.md.us/Press/2008/122408.htm?referer=sphere_related_content

18. Secretary of State Debra Bowen Sues ES&S Over Sale of Unauthorized Equipment to California Counties (11/19/07) Secretary Bowen is suing Election Systems & Software, Inc. (ES&S) for $9.72 million in penalties for selling 972 machines that contained hardware changes that were never submitted to, or reviewed by, the Secretary of State. Furthermore, she is seeking nearly $5 million to reimburse the five counties that bought the machines believing they were buying certified voting equipment. "ES&S ignored the law over and over and over again, and it got caught," said Bowen, the state's top elections officer. http://www.verifiedvotingfoundation.org/article.php?id=6530

19. U.S. Bars Lab From Testing Electronic Voting (1/04/07) A laboratory that has tested most of the nation's electronic voting systems has been temporarily barred from approving new machines after federal officials found that it was not following its quality-control procedures and could not document that it was conducting all the required tests.
http://www.nytimes.com/2007/01/04/washington/04voting.html?pagewanted=1&_r=2#secondParagraph

20. Vendors are undermining the Structure of US Elections (08/2008) A VotersUnite report on the current situation and how to reclaim elections — in 2008 and beyond.
http://www.votersunite.org/info/ReclaimElections.pdf

21.Voting System Companies (NY) Fail to Meet New York State's Requirements for "Responsible Contractors" (7/07) This paper provides fully documented evidence revealing ethical violations include criminal indictments and convictions, civil fines, formal complaints and investigations, as well as consideration of past performance. All of the vendors are guilty of multiple infractions of any notion of responsibility.   http://www.votersunite.org/info/IrresponsibleVendors.pdf

---

"Findings are not accepted by scientists unless they can be verified" Norman L. Munn, (noted author on evolution of intelligence) from American Heritage Dictionary

"Those who cast the votes decide nothing. Those who count the votes decide everything."   Josef Stalin

"Trust, but verify". Ronald Reagan