HELPING AMERICA VOTE

Safeguarding the Vote

In 2002 Congress enacted the Help America Vote Act (HAVA) authorizing $3.9 billion to modernize and improve federal elections. Debate over how to fulfill the requirements of the new law has focused on new technology, both new voting machines and computerized statewide registration systems. Yet, as election officials well understand, new, sophisticated technology alone will not solve the ills that surfaced in the 2000 presidential election. Sound administrative practices are equally necessary to ensure that elections are run both fairly and accurately. And much less has been said on this subject.

According to the law's congressional authors, HAVA is intended to ensure that eligible voters are able to cast a vote and have that vote counted accurately. The law established minimum federal requirements to protect both eligible voters and valid votes, thus providing stronger security for the election process.

In this report, the League of Women Voters focuses not on the technology, about which much has already been said and written, but on the administrative framework that will deploy new technologies and management systems to meet the goals of greater accuracy and security. The report sets forth a set of recommended operational and management practices for election officials that protect eligible voters, ensure valid votes will be counted and bolster voters' confidence.

In "Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues," (2003) a report issued by the Congressional Research Service, three widely accepted elements of defense against security risks are cited: technology, personnel and operations. This League report adopts that framework, but focuses primarily on the latter two elements, personnel and operations. Technological security defenses will be addressed by guidelines developed by the federal Election Assistance Commission (EAC) in cooperation with the National Institute of Standards and Technology (NIST).

In 2002, elections officials in Florida discovered the cost of focusing on technology without equal emphasis on personnel and operations. One county purchased all new electronic voting systems only to discover in the 2002 gubernatorial primary that its process for administering the new machines was flawed — ballots were incorrectly loaded — and its poll workers had not been adequately trained on how to operate the new machines. As a consequence, many polls opened late and some never opened at all.

continued on page two

continued from page one

The same principle holds true with regard to voter registration. Example: In 2000, Florida paid a firm to conduct a computerized match of the voter rolls against felon lists. The resulting list of felons that the state then transmitted to counties for purging had an accuracy rate of only 80 percent. Counties that purged the voters without verifying the information found that they had erroneously removed eligible voters from the rolls. In both cases, technological solutions provided voters no protection against flawed management of that technology.

As states purchase new voting machines and create statewide registration systems, they will need to pay equal attention to administrative and management practices.

This report culls from interviews with election officials and other experts a set of practices that can provide a more secure foundation for two key components of election administration: voting systems and voter registration systems. The recommendations offered below are based on practices already in use. In other words, they are not theoretical but practical. ■

RECOMMENDED PRACTICES FOR ELECTION OFFICIALS

SECTION ONE: VOTING SYSTEMS SECURITY

ACCOUNTABILITY, OPENNESS AND TRANSPARENCY

- Require bipartisan or third-party monitoring of sensitive election procedures.
- Require tracking and documentation of all procedures from the testing of machines to the handling of ballots.
- Require transparency in the operation and management of voting systems.

UNIFORMITY

- Establish statewide practices for the management and operation of voting systems.
- Require that all systems, at a minimum, have been state certified and meet all federal voluntary voting system standards.

TESTING

- Test every voting machine to ensure it is operating properly.
- Perform uniform, public testing of voting systems.
- Verify that the electronic and optical scan machines used are the same as the systems that were certified.

PHYSICAL PROTECTION OF VOTING SYSTEMS

- Restrict physical access to all components of voting systems.
- Maintain and operate voting systems in isolation from networks and the Internet.

PREPARATION PRIOR TO ELECTION DAY

- Educate voters on the use of all voting equipment both in advance of the election and in the polling place on Election Day.
- Provide adequate training for all Election Day workers.

ON ELECTION DAY

- Ensure adequate technical support to poll workers on Election Day.
- Provide a back-up plan in the event of machine failure.

AFTER ELECTION DAY

- Design a routine process that checks for problems that may have occurred but not been visible on Election Day.

SECTION TWO: VOTER REGISTRATION SYSTEMS

- Establish electronic transmission of voter information to the election authority from motor vehicle and other agencies offering voter registration.
- Ensure the registration process enfranchises all eligible citizens.
- Protect voter privacy and database security.
- Require transparency in the administration as well as in the creation of statewide voter registration systems.
- Require tracking and documentation of all changes to the database.
- Conduct accurate voter registration list maintenance.
- Give voters access to review and check their voter record.

SECTION ONE: VOTING SYSTEMS SECURITY

The voting machines on which Americans cast their votes have been called into question. From the now-infamous punch card systems to brand-new electronic voting equipment, voting machines no longer have the automatic confidence of America's voters. While much of the controversy has focused on the voting machines alone, the voting equipment does not constitute the entire voting process. Voting machines function within a larger legal and administrative structure; they are a single component in a larger system. Operational and management issues are very important in the functioning of any system. Many of the risks inherent in the use of particular voting systems — optical scanners, punch card systems, lever machines, and electronic systems — can be substantially reduced by improving such management practices as personnel training and by instituting rigorous administrative procedures. With the November 2004 general elections close at hand and public scrutiny of elections growing more intense, election officials will want to demonstrate their commitment to security. By following relevant best practices that can be implemented in time for the 2004 general election, such as many of those described below, election officials can better protect their voting systems and shore up public confidence in the voting process.

ACCOUNTABILITY, OPENNESS AND TRANSPARENCY

RECOMMENDATION #1: Require bipartisan or third-party monitoring of sensitive election procedures.

A time-honored and effective method to guard against fraud is to open the election process up to bipartisan or nonpartisan scrutiny. Procedures that may be vulnerable or perceived as vulnerable to tampering and manipulation should be conducted under the watchful gaze of partisan and nonpartisan observers. Sensitive election procedures — that is, procedures where cheating might occur — include, but are not limited to, distribution of ballots and deployment of voting systems to polling places; programming and testing of voting machines, including optical scanners; opening and closing the polls; maintenance and trouble-shooting; and the process of counting ballots, including provisional ballots.

The use of increasingly sophisticated voting equipment raises concerns that sensitive election functions will be administered by technology experts, including outside consultants, with little or no oversight precisely because the work is so technical. In the absence of bipartisan technical oversight, election officials may choose to conduct a third-party review of technical processes.

MODEL PRACTICE: In Puerto Rico, representatives from the major political parties play a strong role in almost every aspect of election administration. On Election Day votes are tallied both at the polling place and at the state election headquarters. Both counts are conducted jointly by a team of officials from each of the three major parties.

MODEL PRACTICE: In New Mexico, the state contracts with an independent certified public accounting firm to conduct a thorough audit of the vote counting process. This independent audit follows the state's own audit of all vote totals.

RECOMMENDATION #2: Require tracking and documentation of all procedures, from the testing of machines to the handling of ballots.

Documentation, that is, a thorough and precise record of all relevant operations and procedures, provides the foundation for security in elections. The benefits of sound documentation are two-fold: First, requiring staff and poll workers to record their activities, particularly activities to protect security, helps ensure those tasks get done. Documentation also allows election officials to retrace what happened in the event of a machine or administrative failure. Requiring staff and poll workers to document their actions will allow for an audit to determine whether security measures were bypassed.

Tasks that should be documented include, but are not limited to, the following: receiving and verifying that the correct number of each ballot style has been received from the company printing the ballot; conducting tests to ensure voting machines are running properly; performing scheduled maintenance of all types of voting systems; transfer of ballots or memory cartridges from the polling place to the central office; and any trouble-shooting or repairs on Election Day.

Documentation may not necessarily be paper documentation. For example, a protocol of electronic signatures can track who did what to the machines and when they did it. Some software now allows officials to monitor who gains access to the computer system.

MODEL PRACTICE: In New Mexico, after polls close, the presiding election judge mails to the Secretary of State documentation of the number of voters and the vote totals. The Secretary of State's office reviews the documents, comparing the total voters with the votes cast according to the tapes. Poll workers are required to explain any anomalies. When the county sends the Secretary of State the canvass sheet, the state office compares the machine tapes to the totals on the canvass sheet and investigates any discrepancies.

MODEL PRACTICE: The computer system that administers Georgia's election system incorporates information used to produce a comprehensive set of audit data. For transactions occurring on the system, the system records the nature of the transaction, the time of the transaction and the person that conducted the transaction in an audit log. The audit log allows an investigator to reconstruct the sequence of events surrounding any incident or system failure.

RECOMMENDATION #3: Require transparency in the operation and management of voting systems.

In order to ensure public confidence, the administration of a voting system in its entirety — from purchase to post-election maintenance — should be open and transparent. Election officials must take extra steps to assure voters that not just the systems themselves but the procedures involved in readying systems for Election Day are fully open and accountable.

Certain tests, such as those that verify that machines are running properly — logic and accuracy tests — should be conducted in public. Counting operations such as running punch cards through counting decks and the counting of absentee ballots should be open to public scrutiny as well.

All procurement should be conducted through a bid process that is open to public scrutiny. Reviews and evaluations of various options should be made available to the public. Several jurisdictions formed committees that included technology experts, as well as public interest organizations and stakeholders to evaluate and select new voting systems.

MODEL PRACTICE: Georgia formed a partnership with Kennesaw State University (KSU) to provide in-house expertise in the administration of the state's new statewide uniform voting system including purchase, testing, maintenance, and Election Day trouble-shooting. KSU also helped train the poll workers and educate voters on the new system. The voting systems are tested and approved for use in elections at KSU's Center for Election Systems. The Center ensures the systems meet state requirements and conducts a mock election.

MODEL PRACTICE: Ohio developed a statewide procurement process for the purchase of voting systems using HAVA funds that included a four-phase evaluation of all voting systems. In addition, the Secretary of State kept the public informed at each step of the process, and evaluation reports were posted on the state's Web site. As part of the evaluation, the state hired two independent firms to review the security risks of each voting system. The reports are posted in their entirety on the state's Web site as well.

UNIFORMITY

RECOMMENDATION #4: Establish statewide practices for the management and operation of voting systems.

The scrutiny that occurred during the 2000 presidential election demonstrated the lack of uniformity throughout the nation's election systems. Some jurisdictions experienced voting error rates as high as 30 percent while in other jurisdictions only one or two percent of the votes were not counted. The minimum "uniform and non-discriminatory" requirements established in HAVA were intended to introduce greater uniformity among all election jurisdictions.

Traditionally, while most states have statewide standards for voting systems, the purchase and administration of such systems have been left to local jurisdictions. Local management practices vary widely, leading to disparities in the functioning of voting machines. In the wake of the U.S. Supreme Court's decision in *Bush v. Gore*, however, states have a responsibility to ensure the equal treatment of all votes statewide.

States such as Maryland and Georgia elected to establish a statewide uniform voting system. In Georgia, the state purchased the voting system that would be used in every precinct in federal elections. Every voter casts his or her vote on the same type of touchscreen voting machine. Ohio issued a request for proposals for voting systems and negotiated contracts with four vendors; localities using HAVA funds to replace equipment may purchase equipment only from these vendors. Both approaches recognize that the state now has a responsibility to ensure greater uniformity.

As recent elections have made clear, the management and administration of voting systems can dramatically affect the performance of those systems. Jurisdictions using punch card systems that neglected to keep the vote recorders free of chads experienced problems with votes not registering. Some jurisdictions using electronic systems failed to recharge the voting machine batteries. Other jurisdictions using optical scan systems have run into problems with the scanners' displays when they stored the machines in a room without climate control. These examples demonstrate that all voting systems require diligent maintenance.

States should address this challenge by developing statewide practices for maintaining and administering voting systems and, in addition, providing for uniform testing of all voting systems. Such procedures might include, for example, a schedule for recharging voting machine batteries, physical storage requirements for certain voting systems or required maintenance for

punch card counting decks and other voting systems. In addition, states should develop mechanisms to monitor local compliance.

Procedures associated with poll closing are a critical point in the election process. States are well-advised to have in writing statewide poll-closing procedures that guarantee the process is observable, secure and well-documented.

MODEL PRACTICE: Maryland is developing and implementing a statewide security plan based on a framework recommended by the National Institute of Standards and Technology (NIST) in the publication, "Guide for Developing Security Plans for Information Technology Systems." The state is involving local election officials in the development of the plan.

MODEL PRACTICE: California directs poll workers to post the results for each precinct on the door of the polling place at the close of the polls. These tallies serve as an audit of election night tallies conducted at the central office.

RECOMMENDATION #5: Require that all systems, at a minimum, have been state certified and meet all federal voluntary voting system standards.

Prior to the enactment of HAVA, 38 states required that voting systems meet federal voting system standards. All major U.S. voting systems manufacturers participate in the independent testing process, which qualifies systems according to the federal standards. Once systems have been qualified, the states certify them for purchase or use by localities. Several states impose additional requirements. California, Georgia and Florida, for example, conduct their own certification programs to ensure systems meet state-specific requirements. State certification programs should supplement but not supplant federal testing, standards and guidelines.

If a state requires that voting systems meet federal standards, then the state — as well as the local jurisdiction — has an obligation to prevent bypassing the testing and qualification process. In the 2004 presidential primaries multiple counties used new voting systems with software that had not been federally qualified, a process that includes testing for reliability. According to news reports, a lab hired by the vendor performed only cursory testing prior to the election. The real test came on Election Day when there were not only significant problems with the mechanism for encoding ballots, but the vote tabulating software also attributed thousands of votes erroneously.

While the EAC is developing guidelines for protecting voting systems, states may consider requiring voting system manufacturers to abide by information technology standards already developed by NIST. NIST develops these standards, called Federal Information Processing Standards (FIPS), to fill the vacuum when there are no accepted industry standards. There are FIPS, for example, that address encryption, the security of computer applications and data authentication. Recommendations in the FIPS guidelines for physical security of automatic data processing systems address such issues as preventing access by unauthorized individuals and appropriate climate controls. These recommendations could easily be adapted to voting systems.

MODEL PRACTICE: Ohio issued a statewide Request for Proposals (RFP) from voting system manufacturers and required localities wishing to use HAVA money to purchase new voting systems to purchase only voting systems that have been approved by the state. Ohio required that all voting systems be state certified to meet the federal standards. In addition, the state rigorously tested all potential voting systems, hiring two outside firms to conduct a thorough security review of each system.

TESTING

RECOMMENDATION #6: Test every voting machine to ensure it is operating properly.

Performing tests on every voting machine provides assurances that the system will operate properly on Election Day. This task is time-consuming so election officials will have to plan ahead to allow sufficient time to test every machine. Time spent testing machines prior to Election Day can save time in the end. For example, in a recent primary, a manufacturer technician in one jurisdiction failed to calibrate the optical scan machines to accept ballots marked with a certain type of ink; all ballots marked with that ink had to be recounted.

MODEL PRACTICE: In Georgia, voting machines are arranged by precinct and the memory cards inserted. Each machine is tested to ensure that it is running properly and that the proper ballot information is stored on the machine.

RECOMMENDATION #7: Perform uniform, public testing of voting systems.

This testing should include, at a minimum, (1) logic and accuracy testing for electronic and optical scan systems, (2) testing to ensure the proper ballot has been loaded in the systems, and (3) checking to ensure that paper and optical scan ballots have been properly distributed to the polling places.

Election Day testing and monitoring may also include:

- Verification that the number of voters entering the polling place is equal to the number of votes cast in that polling place. There may be a small discrepancy in these two numbers since sometimes voters will leave the polling place without casting a vote. Nevertheless, this test effectively verifies that ballots have not been fraudulently added.

VOTER-VERIFIABLE PAPER TRAIL: WHAT ARE THE ISSUES?

The Help America Vote Act (HAVA), authorized federal funds to replace poorly-functioning voting equipment. Some have raised concerns about the security of new Direct Recording Electronic (DRE) voting systems — also known as "touchscreen" voting machines and have proposed a particular solution — the voter-verifiable paper trail (VVPT).

Most VVPTs are add-on systems that print out voters' individual ballot choices after they have been cast on the DRE. Proponents of the VVPT argue that this allows the voter to confirm his or her vote and that it provides an opportunity for recounts since the paper record of each individual ballot is retained by election officials.

Because VVPTs are relatively new, federal voting system standards for security, accuracy, accessibility, reliability, availability and maintainability have yet to be developed. Therefore, VVPT systems have yet to be qualified to meet these currently unknown federal standards. VVPT systems also have yet to be widely tested under the rigorous conditions of major elections.

As a potential solution to election problems, VVPT systems deserve and require a close and critical examination. A number of questions have been raised:

- Does the VVPT add security, and if so, how?
- What does it mean to be voter-verified? Does every voter have to verify his or her ballot? What is the value of unverified paper records?
- How will the process of voter verification, whether it is required or optional, be carried out at the polling place?
- What happens if a voter says the paper record is incorrect? 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?
- 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?
- What is the official record of the vote? When will the electronic tally count under the VVPT system, and when will the paper records be relied on? What are the effects of an ambiguous outcome?
- 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?
- What is the effect of the VVPT system on voting access for persons with visual and physical disabilities, persons of limited English proficiency and persons of limited literacy?

The answers to these questions should reflect practical changes to election procedures.

Often the debate over DRE voting systems has been limited to the proposal to require a VVPT. However, a paper trail is not the only means available for auditing the voting process. The Caltech/MIT Voting Technology Project stated that, "an auditable voting system need not be based on paper. Other technologies might emerge in the coming years that would guarantee confidence in election results and would improve on paper ballots in other ways." Caltech/MIT has proposed an alternative solution: separate the vote-recording and the vote-counting processes. This and other approaches, such as instituting a third-party audit, should be explored. Many of the security measures outlined in this report, primarily preventing physical and electronic access to the voting system, would reduce the risk from hacking and manipulation of voting systems. ■

- Parallel monitoring. This test requires randomly pulling voting machines that have been readied for voting — "live" machines — from the polling place on Election Day and testing them to verify that they are accurately recording and tallying votes.

MODEL PRACTICE: In Marshall County, Iowa, election officials perform logic and accuracy testing on each optical scanning device, and perform a hand tally of the test deck. In addition, Marshall County officials employ a written chain-of-custody documentation for all paper optical scan ballots, both to track ballots before Election Day and after they have been scanned and counted.

RECOMMENDATION #8: Verify that the electronic and optical scan machines used are the same as the systems that were certified.

To ensure meaningful compliance with federal and state standards, jurisdictions must develop procedures to confirm that the software being used in an election is the same software that was qualified by an Independent Testing Authority and certified by the state.

MODEL PRACTICE: Georgia tests its voting equipment to ensure that only the certified software has been installed. To conduct this test, the Kennesaw State University Election Center creates and administers a "validation program" that tests whether the software installed on systems at the county level is the same as the certified software. Election officials run this validation program both before and after the election.

PHYSICAL PROTECTION OF VOTING SYSTEMS

RECOMMENDATION #9: Restrict physical access to all components of voting systems.

Election authorities should have systems and procedures in place to guarantee that at no time are ballots, optical scanners, voting machines or records physically vulnerable. Providing such protection may be as simple as storing the computer server in a locked cabinet or it may involve working with the police to provide security for the transportation of ballots. In this context, the voting system encompasses not only voting machines, but also servers and other computer equipment involved in the process of administering the election. Indeed, Section 301 of HAVA defines a voting system broadly as "the total combination of mechanical, electromechanical or electronic equipment (including the software, firmware and documentation required to program, control and support the equipment) that is used to — (A) define ballots; (B) cast and count votes; (C) report or display election results; and (D) maintain and produce any audit trail information." A voting system also includes the "practices and documentation" used to identify the components, test the systems, maintain records of defects and errors, determine any system changes to be made after the system has been certified, and provide materials to the voter.

Providing physical security means restricting access to offices and warehouses storing voting systems. Access to all election facilities should be carefully monitored and controlled.

Providing physical security also means protecting ballots. Election officials should have a plan for managing and documenting the trail of optical scan, punch card or paper ballots, as well as electronic records and paper back-up systems. The plan should aim to allow officials to maintain strict control over the ballots at all times. If feasible, election officials, not poll workers, should take responsibility for transporting ballots from the polling place to election headquarters. Stories abound of poll workers losing ballots or leaving ballots unprotected.

Physical security also encompasses the voting process on Election Day. Neither ballot boxes nor voting machines should ever be left unattended. Even lever machines have physical vulnerabilities: Standing at the back of the machine, it is possible to jam the vote tally mechanism using a device as simple as a paper clip. The mechanism for overriding the error notification feature of optical scanners needs to be protected to ensure that this significant voter protection is not intentionally or inadvertently turned off. Finally, the mechanisms used to end voting are very important and should be protected. Polling place operations should be set up to ensure that poll workers can monitor the voting process.

MODEL PRACTICE: In Georgia, the servers are kept in locked offices within the county election office. No person is allowed access to the computer until his or her identity has been established by the county Election Superintendent. In addition, the PC memory cards in the touchscreen voting equipment are in locked compartments. Only the Precinct Manager has keys.

MODEL PRACTICE: In Virginia and Maryland, the poll workers insert the smart card for the voter to prevent the possibility that a voter might use a "home-brew" generic smart card that could add fraudulent votes to the machine's tally. Smart cards initiate the voting process.

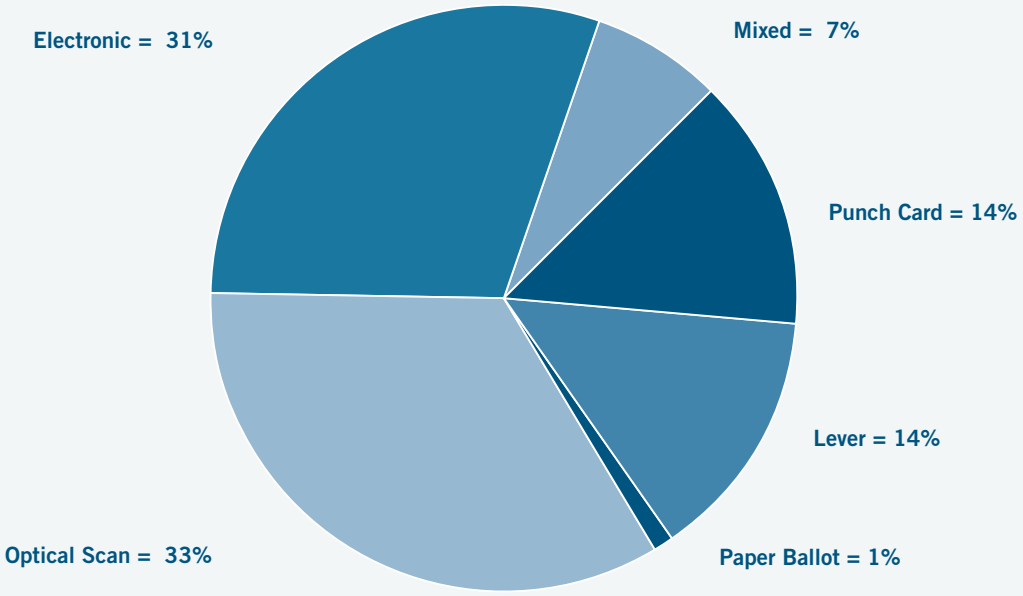
CHECKLIST FOR VOTING SYSTEMS

ALL VOTING SYSTEMS

- Work with design or usability professionals to ensure the readability of the ballots. In particular, the ballot design and instructions should aim to prevent overvoting and undervoting.
- Use only systems that meet federal qualifications and state certification guidelines and standards.
- Educate voters on how to cast a vote properly on their election system, including how to review their ballots, and how to check for overvotes and undervotes. Instructions should be written clearly and simply and provide illustrations.
- Test voting machines and counting machines, including their hardware and software, prior to Election Day. Carry out testing in a public process.
- Educate media, campaigns and elected officials on security measures to protect the voting system and encourage them to disseminate this information to their constituents.
- Ballots, voting machines, memory cartridges and counting machines should never be left unattended.
- Preferably two election officials will oversee all processes, including the transfer of ballots and other election materials to the central office.
- Educate poll workers on how to provide assistance to voters without compromising the secrecy of the ballot.
- Educate poll workers on use of the voting system, including troubleshooting common problems. Poll workers should have a checklist for starting and ending voting on their voting system.
- Do not remove machines from the polls for repairs or for any other reason until voting has ended.

EXPECTED VOTING EQUIPMENT USAGE IN 2004 (PERCENTAGE OF REGISTERED VOTERS)

(SOURCE: Election Data Services, Inc., May 2004.)



CHECKLIST FOR VOTING SYSTEMS

PUNCH CARD SYSTEMS

- Instructions should include directions to check for hanging chads and to review the ballot.
- Provide voters with information regarding what constitutes a spoiled ballot and a clear and no-fault system for replacing a spoiled ballot so the voter can vote on a new ballot.
- Ensure that routine maintenance has been completed before Election Day, including making sure the voting machines are free of chads.

LEVER MACHINES

- Instructions should include illustrations of proper positioning of levers for voting, as well as clear directions on how to write in a candidate and how to cast the vote.
- Ensure that routine maintenance has been completed before Election Day.
- Perform a hundred-vote test count on each machine prior to Election Day.
- Test to make sure mechanism for preventing overvotes is functioning properly.

OPTICAL SCAN: PRECINCT-COUNT SYSTEMS

- If the scanner requires the use of a particular marking device or color, this information should be prominently displayed.
- Provide clear instructions that explain the ballot review process so that voters will feel comfortable correcting a ballot with an overvote or other problem revealed by the scanning process.
- Provide voters with information regarding what constitutes a spoiled ballot and a clear and no-fault system for replacing spoiled ballots so the voter can vote on a new ballot.
- Ensure that scanners are properly calibrated before Election Day.

OPTICAL SCAN: CENTRAL-COUNT SYSTEMS

(also applies to absentee optical scan ballots)

- Voters should receive clear instructions, particularly with absentee ballots. Instructions should be written simply and should include illustrations of properly filled out ballots.
- Both in-person and absentee voters should receive instructions on what constitutes a spoiled ballot and what to do if they spoil their ballot.
- If the scanner requires the use of a particular marking device or color, this information should be prominently displayed.
- Ensure that scanners are properly calibrated before Election Day.
- After 2000, many voters believe that absentee ballots will not be counted unless the election is close. Election officials may want to clarify this process by including a description of the absentee ballot vote counting process and timeframe with the instructions.
- Establish procedures for determining voter intent using uniform vote counting standards and for counting ballots that cannot be scanned. The process for counting ballots should be open and conducted under bipartisan scrutiny.

TOUCHSCREEN VOTING SYSTEMS

- Many of the newer electronic voting systems allow the voter to check if the ballot was actually cast; if so, this process should be included in the instructions.
- Test audio and magnification systems for each machine.
- On Election Day, periodically check to make sure machines are properly calibrated and that cords remain plugged into the socket.
- Double-check to ensure that the device used to encode ballots — the encoder or card activator — has been sent to the proper polling place.
- Configure the polling place to allow full view by poll workers of voting and voter activity to guard against unauthorized access while protecting voter privacy.

RECOMMENDATION #10: Maintain and operate voting systems in isolation from networks and the Internet.

In the debate over the vulnerability of electronic systems to hacking and software tampering, critics have cited the danger of viruses and hacking. Election officials can reduce this risk by maintaining the system in isolation. In other words, no component of the system should ever be connected to the Internet.

Many jurisdictions require unofficial results for optical scan systems and DREs to be sent by modem from the polling place to the central office. According to security experts, the results should be encrypted during the transmission. Even though these election night results are not the official results, discrepancies that show up between election night results and certified results will diminish public confidence in those results.

MODEL PRACTICE: Maryland has implemented cryptographic protocols for all data transmitted via modem. These protocols apply to all systems statewide.

PREPARATION PRIOR TO ELECTION DAY

RECOMMENDATION #11: Educate voters on the use of all voting equipment both in advance of the election and in the polling place on Election Day.

The Caltech/MIT report, "Voting: What Is, What Could Be," found that nationwide 2.5 percent of votes cast were not counted. The number was much higher in some jurisdictions: In some Georgia precincts that used punch card or optical scan systems in 2000, upwards of 12 percent of the votes were lost because of problems with the voting equipment — a percentage that exceeded the margin of victory. Georgia subsequently adopted a statewide system that solved this problem. Their new electronic voting system fully eliminated the possibility of an overvote — the largest source of voting errors on punch card or optical scan voting systems — and reduced the undervote in the top ticket races from 4.8 percent in 1998 to less than 0.9 percent in 2002. Of significant interest were the considerable reductions in overvoting and undervoting in minority precincts. Without replacing voting systems, the number of lost votes can be reduced with thorough, aggressive voter education.

Voters need clear instructions on the voting process. Many jurisdictions conduct extensive pre-Election Day outreach, taking voting systems to malls, grocery stores and community centers to familiarize voters with the process. Hands-on demonstrations are more effective than written instructions. Written instructions are necessary, however, and should include illustrations.

Voters using punch card ballots need to understand that unless the stylus fully punches through the card their vote may not be counted. Voters using precinct-count optical scan ballots need to understand that if the scanner rejects their ballot it may not be counted, and that they should have the opportunity to correct the problem. Voters using electronic voting systems need to understand the process for changing their vote, and that once they have hit "cast ballot," their ballot is irretrievable. And all voters need to understand the ballot, whether it be the layout of a paper ballot or a touchscreen.

Jurisdictions that have replaced their voting systems will find that voter education is key to promoting a successful transition.

MODEL PRACTICE: When Detroit, Michigan, replaced its punch card voting system with a precinct-count optical scan system, election officials undertook a city-wide voter education campaign. The percentage of uncounted votes for president decreased by almost two-thirds, from 3.1 percent in 1996 to 1.1 percent in 2000. Precincts that had over 7 percent uncounted votes in 1996 had less than 1 percent uncounted votes in 2000. Detroit spent approximately $100,000 on voter education, taking systems out into the community, conducting daily demonstrations at community centers, churches, festivals and government buildings. The city also produced public service advertisements for television, radio and billboards, and blanketed the city with flyers and pamphlets.

MODEL PRACTICE: Montgomery County, Maryland, and Los Angeles County, California, both provide live-streaming video instructions on the voting process on their Web sites.

RECOMMENDATION #12: Provide adequate training for all Election Day workers.

On Election Day, the voting system lies in the hands of poll workers. The importance of adequate poll worker training, therefore, cannot be overemphasized. Poll workers must be trained to ensure the physical security of the voting system, to start and end the voting process correctly, to assist voters who may have difficulty voting, and to protect the voter's privacy.

Poll workers need to understand the security vulnerabilities in order to effectively guard against security breaches. They need to understand the purpose of the

optical scanner's error notification features so they can explain it to the voters. Poll workers need to be trained on how to close down the poll properly and document the vote tallies accurately.

After the 2000 presidential election, Florida overhauled its election system, replacing voting systems in 2002. As most election officials remember, two counties experienced serious problems when new systems made their debut in the 2002 primary.

On September 20, 2002, the Miami-Dade Inspector General (IG) issued a report following an inquiry into circumstances surrounding the primary election. While the IG's report faults problems with the voting systems and with administrative planning, the report also focused on the inadequacy of poll worker training.

Beyond the problems poll workers experienced with equipment, two reports, including the IG's report, noted that poll workers did not have a clear understanding of basic procedures. The problem did not lie with the poll workers themselves, "… the matter does not lie in the caliber or technological experience of the poll worker, but is grounded in the absence of quality training sessions and written training materials," the IG concluded.

MODEL PRACTICE: In Los Angeles County, California, election officials are preparing for an eventual transition to electronic voting systems by actively diversifying the poll worker workforce, and by recruiting tech-savvy municipal employees, students and private-sector volunteers.

MODEL PRACTICE: Maryland's statewide security plan requires training Election Day workers, "election judges," on the security procedures outlined in the plan. In addition, the state will also train other key Election Day officials, including local election officials and staff on the new plan.

ON ELECTION DAY

RECOMMENDATION #13: Ensure adequate technical support to poll workers on Election Day.

While many election officials rely on the voting system manufacturer to provide technical support on Election Day — provided they included such service in the contract with the vendor — they also need a plan in place to supplement the manufacturer's support with independent technical support. Such a plan would likely provide tiers of technical expertise ranging from a troubleshooting checklist at each polling place to manufacturer technical support. The aim is to reduce the burden on the response system by giving poll workers the tools to fix routine problems themselves.

To reduce the reliance on voting system vendor support over time, election officials should plan on developing their own in-house expertise. Election administrators may consider developing a cadre of trained professionals to handle the demand for technical support on Election Day. This cadre of technicians would be available either to resolve problems over the phone or to go to the polling place. Knowing how to operate a computer does not qualify as adequate technical expertise. The technical support personnel must understand the larger administrative process as well.

The support plan must not only cover ensuring the availability of technical support, but also a communications strategy to guarantee that poll workers can access that support. A common sense solution is to provide a hotline for poll workers on Election Day — and to make sure the hotline is adequately staffed!

Jurisdictions may wish to consider conducting an assessment of poll workers' comprehension and comfort level with basic operations and troubleshooting to ensure they have adequate knowledge to carry out their duties.

MODEL PRACTICES: The District of Columbia Board of Elections recruited, trained and deployed "precinct technicians" to help poll workers and voters operate new electronic voting equipment. Following a trouble-filled primary in 2002, Miami-Dade County, Florida, brought in computer specialists from other county agencies to provide Election Day support to poll workers. Likewise Montgomery County, Maryland, called on county information technology workers to assist at the polls on Election Day.

RECOMMENDATION #14: Provide a back-up plan in the event of machine failure.

The reality of technology is that individual machines — individual touchscreen units, ballot encoders, scanners — will fail. And when that happens on Election Day, whether the result of human error or machine error, voters can be disenfranchised. Accordingly, there must be a back-up option. In jurisdictions that use DREs, additional machines should be available in the event of machine failure. In other jurisdictions, additional ballots should be available in case sufficient ballots did not arrive at the polling place.

AFTER ELECTION DAY

RECOMMENDATION #15: Design a routine process that checks for problems that may have occurred but not been visible on Election Day.

States may conduct an audit of the election after Election Day to provide the public with additional assurance that all votes were counted properly and accurately. This practice may also alert election officials to problems that occurred that may not have surfaced on Election Day.

MODEL PRACTICE: In New Mexico, poll workers keep duplicate copies of all documents, such as machine tapes, poll books and hand tally sheets. These documents are mailed separately to the state election office. After the state's canvass, an independent certified public accounting firm conducts an audit of the entire election, checking the documents received from the poll workers against those received from the local election officials. Any discrepancies are investigated.

SECTION TWO: VOTER REGISTRATION SYSTEMS

When Congress first began looking into the election system following the 2000 presidential election, it soon became clear that poorly administered registration systems posed a bigger problem affecting more voters than antiquated voting machines. Eligible voters were disenfranchised because their registration applications were not being processed and because of other systemic problems. Ten years after passage of the National Voter Registration Act (NVRA), some states and localities had not yet found an efficient, reliable means to transmit voter registration applications from motor vehicle and other agencies, which are required to provide such applications to citizens, to the proper election authority.

In Section 303 of HAVA, Congress mandated that states establish a statewide computerized voter registration list in order to address these types of problems. Forty-four states requested waivers from this new requirement and are therefore not required to implement this provision until 2006. The design of these statewide computerized registration systems is key to establishing a well-administered election process.

RECOMMENDATION #16: Establish electronic transmission of voter information to the election authority from motor vehicle and other agencies offering voter registration.

A well-run registration system will provide an electronic link between the election agency and the agencies specified in NVRA as registration agencies, including agencies serving persons with disabilities and public assistance agencies.

Electronic transmission is timelier and more accurate than physical transmission. In Michigan, the information is transmitted instantaneously since the motor vehicle and the election authority share the same database. Electronic transmission also eliminates the need to enter the data a second time, thus reducing costs and minimizing the opportunity for clerical error.

Jurisdictions that transmit voter information from one agency to another electronically are much less likely to experience registrations falling through the cracks. Conversely, voters in jurisdictions that still transfer paper applications are far more likely to show up at the polls believing they have registered, only to find their names are not on the list. States that fail to provide for electronic transmission will likely have far more provisional ballots, increasing their post-election administrative burden. A majority of Los Angeles County's provisional ballots are cast by voters who registered at the motor vehicle agency but whose registrations either got lost in the system or were not processed in time.

MODEL PRACTICE: Michigan's Qualified Voter File is a unified database shared by the state election agency and the motor vehicle agency. Changes and updates made to the voter registration record are automatically made to the driver's license record, and vice versa (in Michigan the address for voter registration and motor vehicle registration must be the same). Electronic transmission allows new registrations and updates to be processed in real-time and significantly reduces the likelihood of losing applications in transmission.

RECOMMENDATION #17: Ensure the registration process enfranchises all eligible citizens.

The voter registration process can assure good administration of the election process, or it can serve as a barrier to voter participation. The design and implementation of a statewide computerized voter registration system holds great promise if it is properly designed to ensure enfranchisement of all eligible citizens.

In creating a statewide database, states must establish where responsibility lies for adding, deleting and updating voter records and specify, in law or regulation, the rules for determining both eligibility and ineligibility.

States must assign each voter a unique identifier, a change that will significantly reduce the deadwood on voter lists over time by allowing states to track voters as they move within the state. State election officials can either create their own system by assigning randomly generated numbers to each new voter or piggy-back on another system such as the motor vehicle agency numbering system.

In establishing rules for the voter registration process, the state should ensure that information is used to complete accurate registrations, rather that setting up obstacles to the voter registration process. For example, if a voter registration applicant fails to provide a driver's license number or inadvertently transposes numbers, the database system should help correct that application so it can be processed and accepted. The state should have a transparent administrative process that includes information on the acceptance or rejection of applications.

HAVA requires that a voter registration application include the driver's license number, or the last four digits of the SSN if the applicant has not been issued a current and valid driver's license. The appropriate number can be provided by the applicant or by the state's databases. The chief state election official and the official responsible for the state motor vehicle authority are required to enter an agreement to match data, and the motor vehicle official must enter a similar agreement with the commissioner of Social Security.

As HAVA is silent on how states should treat the results of this database matching, states must determine how to conduct these matches as well as what to do with the results. According to the Social Security Administration (SSA), at least ten percent of the information obtained as a result of matching the name and last four digits of the SSN will likely be inaccurate. Two types of errors may result: First, matching the last name and the last four digits can produce multiple apparent matches, called "false positives." In addition, errors such as inaccurate

PURGING OF VOTER LISTS

In 1993, Congress passed the National Voter Registration Act (NVRA) to expand the opportunities for eligible citizens to register to vote. In addition, the NVRA encouraged states to coordinate voter records with other databases in order to keep lists accurate and up-to-date. At the same time, however, the law also established safeguards to prevent eligible voters from being erroneously purged.

HAVA adopts the NVRA list maintenance standards. Nothing in HAVA alters the requirements under NVRA to protect voters from erroneous purges.

The consequences of flawed list-cleaning procedures were clearly evident in November of 2000 when thousands of Florida voters found themselves unable to vote after they had been purged from the rolls based on erroneous information sent to county election officials by the Secretary of State.

In 2000, the Florida Secretary of State's office contracted with an outside firm to match voter registration records against felony records. Not only was the underlying data from the Florida Department of Law Enforcement unreliable, but the matching criteria were so broad that thousands of eligible voters were erroneously tagged as felons. The resulting match had an error rate of approximately 20 percent. Despite the inaccuracy of the information, the state made the data available to the counties and encouraged them to use the information to purge the voting rolls.

Several counties then purged voters from the registration records without bothering to verify the accuracy of the information.

The lesson from Florida is simple: database matching to remove felons, deceased voters and duplicates, cannot, in itself, substitute for an accurate verification process. Accordingly, states and local election officials must build sufficient time into the list-cleaning process to conduct proper verification. And the reliability of the underlying data should always be checked before it is used. (See page 16 for details of the settlement agreement between the state of Florida and the NAACP.)

Still, even using stricter standards, database matching is not foolproof; further verification is advisable. Providing notice to the voter before any purge is carried out allows that voter to correct an error before it results in erroneous purging. ■

name spellings and transposed numbers can result in the appearance of no match.

Given this high rate of inaccuracy, it would be a mistake to reject voter applications when there is no identical match; doing so would almost certainly result in disenfranchising eligible voters. In the event the attempt to match produces no match, states have the option of assigning a randomly-generated unique identifier. In the event that a database match produces information suggesting ineligibility, such as when the voter's last four SSN digits and name correspond to someone who is deceased, states should develop procedures for following up with the applicant to verify the information. (See "Purging of Voters Lists" for a more detailed discussion of the challenges involved in database matching.)

Matching with motor vehicle records poses other difficulties: addresses are likely to be different; driver's license numbers may be accidentally transposed by the applicant; and the types of data may be different. All of these indicate the need for officials to use DMV data to supplement the registration process rather than use it as a reason to reject an applicant. To resolve inconsistencies, election officials will need to follow up with the voter by mail or other means.

Election officials would be well-advised to study the matching process, particularly at the beginning, to determine the reliability of the information received from either the motor vehicle agency or the SSA.

While HAVA gives the state responsibility for defining, maintaining, and administering the official voter registration list, local registrars will likely retain responsibility for important steps in the process. A well-run registration system will necessarily involve close cooperation between state and local offices. States must spell out the details of processing voters and take steps to ensure the procedures are followed uniformly throughout the state.

MODEL PRACTICE: In California, the state searches the motor vehicle database to pull the driver's license number, which then is added to the voter record. The state also compares voter records to health records. The practice not only helps the voter, it also ensures more accurate records.

RECOMMENDATION #18: Protect voter privacy and database security.

HAVA requires that the appropriate "State or local official shall provide adequate technological security measures to prevent unauthorized access to the computerized list…" States therefore must establish strict rules for administering the database and ensure each locality adheres to those rules.

Creating a protocol for access to voter records should be part of establishing a regulatory framework for administering the database. This protocol would create hierarchical levels of access to the database, giving certain users discrete authority to perform certain tasks. Not all election staff have authority to perform the same functions. Very few staff, for example, would have authority to remove names from the list.

On the one hand, of course, the registration list will be a very public document: Almost every state allows political organizations and parties to purchase the list, which contains voters addresses, party affiliation and voting participation history. On the other hand, information such as the voter's driver's license number or SSN requires strong protection. The database must be structured in such a way as to accomplish both goals.

As with the administration of voting machines, thorough and rigorous documentation of all operations is necessary to ensure public confidence in the security as well as the accuracy of the list. List administrators must be able to track who has accessed the list as well as what transactions, such as updates and additions, have been performed, and when.

Protecting database security includes providing physical protection as well. Moreover, the server should be in a protected location that does not offer public access.

MODEL PRACTICE: In Michigan, local election officials have authority to add, delete and update voter records; however, any change must ultimately be approved by the state in order to be made official. Michigan also has in place rules governing which employees can perform which tasks.

MODEL PRACTICE: In the District of Columbia, the chief technology officer can monitor both successful and unsuccessful attempts to enter the voter registration database. In addition, all users are now required to change passwords on a monthly basis in order to prevent former employees from gaining access or allowing others to gain access to the database.

RECOMMENDATION #19: Require transparency in the administration as well as in the creation of statewide voter registration systems.

A computerized voter registration system is more than just a database — the details of its creation and administration will determine if and how well the rights of eligible citizens are protected. Many states are seeking consultants to help them write the "request for proposal" for technical assistance in constructing the registration system; some states are developing the database themselves. In either case, the process for designing the system should be public and transparent. It should involve stakeholders, including the local election officials, parties, voter advocates and the public. These stakeholders should have a voice in defining the system — particularly the procedures for adding, deleting and modifying records.

In many states, involving local election officials at the beginning of the process will reduce the likelihood of problems when it comes time to implement the system. Such officials bring a practical understanding of the registration process and will have insight on the details of the system's construction.

States may divide up the administrative work between state and local officials differently. For example, in Michigan the localities submit voter information to the state that has ultimate authority for adding and deleting voters to the database. In Kentucky, the state has authority to remove registrations while localities have authority to add and update registrations. In the end, however, the state has sole responsibility for the system and for ensuring its accuracy.

MODEL PRACTICE: Pennsylvania made both the initial study of what would be required to create a statewide list as well as the RFP publicly available. Soon after Pennsylvania began implementing its statewide system, the state contracted with a private firm to review and evaluate the implementation process. The firm conducted a thorough review of the system and made dozens of recommendations for improvements. The state posted the report on its Web site.

RECOMMENDATION #20: Require tracking and documentation of all changes to the database.

States should have a method for monitoring all changes — additions, deletions and updates — made to the list. This monitoring might include electronic signatures within the database or it might include a requirement for thorough documentation.

MODEL PRACTICE: In the District of Columbia, the voter registration database tracks who made changes — additions, updates, deletions — to the voter registration records.

RECOMMENDATION #21: Conduct accurate voter registration list maintenance.

Elections are a unique governmental function; the use of database technology in election administration will require different procedures and more stringent safeguards than in other areas of government.

Nothing in HAVA allows election officials at the state or local level to bypass protections intended to prevent voters from being disenfranchised for administrative errors, specifically, the protections for voters established in the NVRA. Under NVRA, election officials are prohibited from removing a voter who they believe has moved unless the voter confirms the information in writing. Nothing in HAVA alters this safeguard.

Even if it appears that several records belong to a single voter — who has moved from one jurisdiction to another and registered after each move — the election official cannot remove any of the apparent duplicates without written confirmation by the voter.

NVRA requires states to perform list-cleaning procedures to keep voter registration lists current and accurate, including obtaining data from other sources such as the National Change of Address program, death records and felony records. While this data can provide useful information, it must always be verified. Stories abound of people who have died continuing to receive Social Security checks posthumously and, conversely, people still very much alive erroneously being included among the dead. One jurisdiction in 2000 matched the voter list against a tax assessor's list and required voters whose addresses did not match the assessor's list to vote by provisional ballot at the central election office. However, the assessor's list was ten years old, and some of the addresses identified by the assessor as invalid or "vacant lot" had since been developed into residences. Voters should not be penalized for inaccurate or out-of-date record keeping.

The polling place on Election Day can be a key point in the list-cleaning process if voters are allowed to update their registration information when they come in to vote. Poll worker training should, therefore, include easy-to-follow guidelines on how to note change of address, spelling corrections and other changes. Election officials must be vigilant in following up on this information.

MODEL PRACTICE: The following rules for determining multiple registrations, sometimes known as "duplicates," were taken from the settlement agreement between the state of Florida and the NAACP. Following this model will guard against faulty matches.

To determine multiple registrations, the state may match:

- the last name, first name, least common denominator of the middle name, and the date of birth (DOB);
- full nine digits of the SSN, last name, and either first name or DOB;
- driver's license or state ID number, and last name;
- SSN and last name, or DOB; or
- Florida ID and last name, or DOB.

In applying these matching criteria, the following conditions apply:

- the last name in both records must be exact;
- the DOB in both records must be exact;
- there can be no conflict in race data or gender data; and
- there can be no conflict in SSN — transpositions will not be accepted.

Of course, the data that is matched against the voter registration list must be accurate.

RECOMMENDATION #22: Give voters access to review and check their voter record.

Voters can and should be a part of the process to ensure the accuracy of their voter record. Voters should be able to view their registration information in order to check the accuracy of the address, party affiliation, voting jurisdiction, polling place and age.

In smaller jurisdictions, voters can call the registration office to obtain their voter information. In larger jurisdictions, the administrative burden can be reduced by making a copy of this information available on a Web site.

Encouraging voters to check their registration information for accuracy prior to the deadline should allow for a reduction in the number of provisional ballots cast during an election. The more voters who can straighten out registration problems prior to the election, the fewer voters whose eligibility will be in doubt on Election Day.

MODEL PRACTICE: Virginia's elections Web site allows citizens using a personal identification number to view their voter registration information, including their proper polling place, online. Voters do not view this information directly in the database, but review a public copy of this information.

LEAGUE OF WOMEN VOTERS®

1730 M STREET NW
WASHINGTON, DC 20036
TELEPHONE 202.429.1965
www.lwv.org

WRITTEN BY TRACY WARREN
IN COLLABORATION WITH LLOYD LEONARD, JEANETTE SENECAL AND KELLY CEBALLOS

PUB#2065