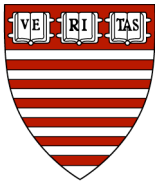

Voting, Vote Capture & Vote Counting Symposium

June 2004

Kennedy School of Government
Harvard University

Electronic Voting Best Practices

A Summary

Acknowledgements

The following document was developed by Jean Camp, Allan Friedman and Warigia Bowman of the Kennedy School based on the *Symposium on Voting, Vote Capture & Vote Counting*. Other contributors include Dr. Rebecca Mercuri, Lillie Coney of the National Committee for Voting Integrity, as well as members of the Open Voting Consortium particularly David Mertz. Many participants contributed notes and comments during the development of this summary. Rebecca Mercuri also assisted with organization of the event.

Professor Camp can be reached at jean_camp@harvard.edu or 617-233-6658.

The attendees for this event included technologists, election officials, political scientists, policy analysts, notable press experts, and activists. Despite the diversity of opinion, the event was characterized by serious discourse and learning across domains.

The Symposium began with two sets of speakers. The speakers who described logistical and organizational challenges were Thad Hall, Mary Kiffmeyer, Al Lenge and Connie McCormack. David King moderated the panel and assisted in reviewing the summary.

The speakers on the panel describing the technologies of voting were Rebecca Mercuri, Lorrie Cranor, Ron Rivest and Avi Rubin.

Not every speaker and contributor need agree entirely with every best practice, as the speakers did not entirely agree with each other.

A list of documents providing an overview for further reading on the state of elections technology is available at the Symposium web site, http://www.designforvalues.org/voting

This is a summary document, reflecting the overall sense of the workshop.

Support for the Symposium was provided by the National Science Foundation and the Kennedy School of Government. A gift to support

Rebecca Mercuri's work in verified voting to the Kennedy School provided partial funding for the event.

Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation, Harvard University, the Kennedy School of Government, all participants or views of the National Science Foundation, Harvard University, the Kennedy School of Government, all participants or funders.

Annotated Best Practices

The following is a set of annotated best practices are written as a summary of the Symposium. Although not every Symposium attendee will agree with every best practice, this document are intended to reflect the overall sense of the event.

One goal of the symposium was to setting out for contemplation and discussion the major issues involving vote collection and tabulation. In this vein there were six major themes that emerged in the discussion in the symposium. First, there is a need for immediate steps, and long term systematic organization. Second, a hybrid system that includes paper for audit and electronics for speed and flexibility is an effective option. Third, there is a critical need for investment in the human element. Vote tallies can be speedy or accurate, but not both, and the public should understand this very human distinction. Fourth, design standards are needed for all technologies – including paper ballot with respect to usability. Fifth, transparency in processes, including electronic processes, is critical. Sixth, electronic systems require an audit trail consisting of independent non-aggregated artifacts of which paper ballots are the only currently feasible option.

1. Certain Immediate Steps Must Be Taken.

The symposium on voting and technology identified some key themes that ran throughout our discussions, and which will be highlighted in this document. However, with the 2004 Presidential election fast approaching, it is important to prioritize issues related to voting technology. Certain actions can and must be taken now, both for 2004 and beyond.

1.1 Election Assistance Commission and National Institute of Standards and Technology open standards must be developed and implemented.

The Help America Vote Act (HAVA)[1] provides funds, which are heavily subsidized by federal grants awarded providing for both the newly formed US Election Assistance Commission, and for the election-related purchases, including the purchase of machines. The function of reviewing voting technology and development of standards under HAVA was assigned to a Technical Guidelines Development Committee (TGDC). Under the proposed leadership of the Director of the National Institute of Standards and Technology (NIST),[2] the TGDC can take significant steps toward the development of rigorous testing and certification processes for electronic voting technology. Unfortunately, efforts to develop and implement standards have been hindered by lack of funds and a slow start to the process. The standardization process must be well-funded, include qualified experts, and as timely as possible.

EAC and NIST voting standards must be open and freely implementable. Anyone should be able to gain access to these standards to ascertain how much security they guarantee, or whether a specific technology is in compliance. They must be freely implementable so that any qualified organization can design a system that meets EAC standards. This not only aids in ensuring a competitive market and thus responsive vendors; it also can help with popular perceptions of trust.

1.2 Voting experts and technologists can aid in whatever voting process is used by designing guides, working in polls and gathering trustworthy data.

---

1 Help America Vote Act of 2022 (HAVA), Public Law No. 107-252, 116 Stat. 1666, available at http://www.fec.gov/hava/law_ext.txt

2 National Institute of Standards and Technology http://vote.nist.gov/faq.html

As advanced technology is increasingly used in elections, the need for computer literate participants in the process is critical. Information technology experts from across state and local government should be made available to voting officials.

The current process for evaluating technical decisions about election purchases is often flawed. The current processes often require election officials to place a high degree of trust in vendors. Even in the case of trustworthy vendors, such trust is inappropriate in democratic public voting technology. In addition, independent auditing organizations should be truly independent.

2. A Hybrid Of Paper And Electronic Systems Provides An Effective Voting System.

No technology can solve every problem and mitigate every risk. Neither electronic nor paper ballots are a panacea. A hybrid of paper ballots and electronic systems can capture the benefits of each while avoiding the pitfalls inherent in relying on one or the other. The ideal system depends on the best attributes of each, and uses modular construction that allows for simple integration of the two parts. Of course, if badly implemented the combination of electronic systems and paper ballots can offer the problems of both, instead of benefits. An example of a hybrid is the Massachusetts optical scan system, which has paper ballots with electronic system to tabulate. Another alternative is paper ballots with electronic marking systems. (Note that HAVA does not require the purchase of electronic system components.)

Voting is particularly difficult technical design challenge because voting is anonymous. Auditing in digital transaction-based systems is usually implemented by tracking an identity-based record, such as a bank account, and providing receipts. Auditing in voting must be done anonymously. Paper can provide anonymous auditing for each voter.

2.1 Electronic interfaces enable customizable ballots by precinct, party or disability.

An advantage of electronic vote-selection systems is that a programmable interface is fully adaptable to a wide range of needs. Such flexibility can accommodate local or individuals needs, as well as particular demands of a given election. From a cost perspective, it may be cheaper for a larger jurisdiction to customize the interface for voters than to distribute separate ballots to appropriate precincts in appropriate languages with appropriate features (e.g., print size). Generation of ballots on a per-user basis can greatly simplify the remarkable logistics problem of matching each voter with an appropriate ballot. An electronic interface can also offer interactivity and help the voter to cast the ballot he or she intends.

A smart system can check for undervotes or overvotes and can inform the voter that the ballot may be recorded as such, in time for the voter to alter his or her selection before creating a finalized ballot. For example, precinct-based optically scanned systems can flag undervotes and overvotes before the voter departs.

The flexibility of electronic interfaces does not mean that they are optimal, or even usable. For example, the widely criticized butterfly ballot could easily be reproduced on a screen. Translating an interface's flexibility of interface design into usability requires a process that includes usability testing

It is critical that ballot customization is implemented in a privacy-enhancing manner. Ballots that are customized to the individual, as opposed to customized interfaces, can uniquely identify individuals. For example, only one person voting in a particular district may speak a particular language or have a particular disability. Note that such a hybrid may include a flexible optical character recognition (OCR), an audio multi-lingual ballot reader/marker, or a paper ballot-generating Digital Recording Electronic device (DRE).

2.2 Electronic Interfaces can meet the widest range of accessibility needs.

In any configuration, language and special need ballots increase the necessity of complete usability testing. All possible ballot configurations should be tested before placing the voting system in the field. The existing Federal accessibility guidelines and the Web Content Accessibility Guidelines (http://www.w3.org/TR/WCAG10/) offer a starting point; but neither standard assures usability in practice.

Recent tests and interviews have shown that many people prefer using an electronic interface in the voting process. Voters' comments regarding their experience using voting machines with electronic screen interfaces are reported as being "great," "very easy," and "fast".[3] Moreover, the customizability means that language does not have to be an impediment. In contrast, some users are disoriented by screen-based systems. Users without bank accounts or elderly users can be confused by the ATM-style interfaces.

Screen-based systems do not have inherent value for the severely visually impaired because they depend on a visual interface. An audio interface or tactile ballots can empower visually impaired voters who cannot interact with screens.

A set of appropriate, usable paper ballots can be used with an OCR. Such ballots can be augmented with ballot-reading devices. OCRs are flexible electronic devices, can tally different ballot configurations, and the system's few components enhance usability.

---

[3] McCaffrey, Raymond and Barr, Cameron W. "Debut of New Technology Gets Mostly High Marks" The Washington Post. Found at: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A24780-2004Mar2&notFound=true March 3, 2004; Page B04

2.3 Voter verification of a paper ballot allows the greatest degree of confidence that the ballot was cast as intended.

A paper ballot can be visually or possibly physically examined by the voter, which offers a greater degree of confidence. A human-readable ballot allows the voter to be certain that the ballot being counted was what the voter intended. The voter should be able to void his or her ballot and start anew if necessary.

To ensure privacy and prevent the generation of records, under no circumstances should the voter be able to leave the polling place with a ballot containing evidence of the vote.

Additional mechanisms to read and verify the ballots can ensure the privacy of voters with special needs; automatic auditory ballot readers for the visually impaired, for example. If machine-readable information such as bar-codes exist on the ballot, electronic readers should be made available so that the citizen can interpret them.

2.4 A paper ballot, when handled properly, allows a robust audit trail for a recount to ensure that the ballot was count as cast.

As discussed below, auditability is a crucial component of any election. An electronic or mechanical system that provides only final election tallies cannot be audited. A meaningful audit requires the availability of independent non-aggregated artifacts that are highly resistant to tampering. Properly handled paper ballots are well-suited for this purpose. Moreover, because paper ballots can be counted by hand, electronic counting machines are not essential for performing audits.

2.5 Hybrid systems can be designed to accommodate provisional arrangements and contingencies for equipment failure.

There are many possible implementations of a hybrid system. If auditable ballots are available at the polling place, then voters can still

cast their ballots directly on the voting stock. Voters of unknown registration status can still cast their vote using the same system as others, and their eligibility can be confirmed before the ballot is entered into the final count.

A hybrid system could revolve around an Optical Character Recognition (OCR) engine with a ballot reader and a ballot marker. Alternatively, a general-purpose computer with a printer could satisfy many needs, as could a standard DRE with a printer. A popular option is a multi-stage architecture with complete separation between casting, validating and submitting votes for count. (Since this has not been used in practice research, testing and pilots for unanticipated problems would be needed.) Another alternative is paper ballots marked by voters with interfaces for special needs voters.

3. The Process Is As Important As The Underlying Technology.

The process of executing the election is at least as important as the underlying ballot technology. Perfect technology cannot repair a fundamentally flawed process. Adequate policies, institutions and people are needed to make sure that the voting systems are properly used. In every electronic technology, particularly security technologies, the human factor is a critical component.

The process and people require investment as least as great as the investment in the technology. There are certain inherent trade-offs in the process that the technology may obscure but does not resolve.

The emergence of election administration as a profession, including the maturation of professional associations, is worthy of support. Other options include creation of professional guidelines, certification, training or testing for those who are in public positions with the responsibility of administering elections. International interaction of election officials can support the creation of a knowledge base. Many other nations have trained, civil-service election administrators to guarantee a non-partisan process.

3.1 Poll workers should be well trained to fully understand the interface and contingency plans in case of failure.

The poll workers are the voters' first and, in most cases, only assistance in navigating the voting process. When introducing new technology to the polling place, the poll workers must be well-equipped to assist the voters in any way, as well as prepared to respond to any problem that may arise. Training the poll workers is a large undertaking, as is training the officials who will be teaching the poll workers. These time constraints must be reflected in the schedule of deployment for any new system. Poll workers must be aware of what they might face and given the tools to address as many of them as possible. This includes understanding how the systems are to be operated in special cases, such as power failure, provisional voting and voters with special needs.

3.2 The educational process for given technologies must follow a "chain of trust" where the election workers trust their trainers and are trusted by the public.

If the voting system is not understood or trusted by the poll workers, they will not be able to adequately serve the public. All those participating in the election management process must have a good understanding of how the voting system works, and how each component helps ensure a well-run election. One major concern is the generational gap between the poll workers who volunteer and the professionals who maintain the computer equipment that may be foreign to the volunteers. Poll worker training must be designed to address this concern, and try to minimize discomfort or worries. The needs of poll workers should be considered in the design of any voting technology.

3.3 Poll workers should be well-chosen from a motivated pool with appropriate incentives.

It is not enough to train poll workers; they must be motivated, responsible and competent.

A very effective public relations campaign could be generated to increase the desire of registered voters to work at polling places on Election Day. Athletes, musicians, actors, etc, can be enlisted as Election Day workers. A target goal may also be higher voter participation by younger voters. A pilot project would be effective in testing out ways to improve the response to the community need of poll workers to service in local elections

One option is an adaptation of the jury pool system currently used to satisfy the legal requirements of jury trials. Such an adaptation would rely upon voter registration lists and could be modified for a new poll worker pool program. Those participating in any poll worker pool would receive monetary compensation for two days, which should include one day of training and Election Day. In addition, poll workers could receive some number of years of exemption from both jury service and poll duty. As an incentive those who volunteer could receive five years of exemption from jury service or poll duty.

Another alternative, one that has proven successful in New York, is to directly recognize the value of poll workers with increased and generous payment. Payments on the order of hundreds instead of tens of dollars allow election officials to choose from competitive poll worker applications.

3.4 Poll workers should not have to rely solely on the vendors to address observed errors.

Open or standardized systems should allow local officials or an independent contractor to intervene when necessary. Trade secrets or contracts should not prevent dissemination of information for failure

recovery, error recognition, or contingency plans. Reliance on the vendors can create conditions for lock-in, if the jurisdiction is dependent on the vendor.

There should be a record of failure information available to election officials, and poll workers should be able to enter and record their own difficulties into this shared record. Such a knowledge management system could allow poll workers and jurisdictions to share innovations as well as difficulties.

3.5 There should be adequate time for determining the official tally.

It is critical to make sure every vote counts. Provisional ballots may need to be evaluated and added, and the process should be assessed after the fact for irregularities. Audit should take place soon after the election, and should be comprehensive. The unofficial returns may be released soon after the election; but time should be taken with the official tally.

Paper ballots can provide trustworthy, reliable official tallies.

3.6 Speed and accuracy in the process are both achievable, but not simultaneously possible.

Fast counts necessarily exclude provisional votes; may not include time to examine ballots for undervotes; and cannot provide time to adjudicate contested results.

The public should be educated about the distinction between the speed that allows immediate returns, and the accuracy required in the official tally. Electronic systems can provide speedy counts.

There is no way to get a guaranteed fast tally, which is a count that is as accurate, as possible. The public must understand that every vote counts, and should be counted. Promises or expectations of quick resolutions should be avoided, and the media should not overly stress preliminary counts. If a preliminary, uncertified tally is spread

publicly, then contradicting that news can decrease confidence in the election. Distributions of preliminary counts should be identified as preliminary in all cases.

3.7 There should be provisional voting mechanisms, and adequate time to evaluate provisional votes for the final tally.

Full information should exist about voter eligibility, but it is not always easy to get that information to the polls, and for that information to be up-to-date. Moreover, sometimes voters dispute their disenfranchised designation, and should have the ability to vote provisionally if the matter can be resolved in the matter of days. Those who avail themselves of provisional ballots should have access to the other features of the voting system, including accessibility and verifiability tools.

HAVA directs the use of provisional ballots, but it is silent on their evaluation for the final official count. It is not sufficient to allow for provisional voting if there is no mechanism for determining the disposition of those ballots. Jurisdictions require rules and procedures for the determination of which ballots will be counted. The U.S. Election Assistance Commission and U.S. Civil Rights Commission could assist by providing process standards and advice to jurisdictions on the best course of action regarding the dispensation of provisional ballots.

3.8 There is an inevitable tradeoff between authentication of voters and access.

Requiring greater proof of the right to vote will prevent some from voting; removing any requirement for proof will allow those without the right to vote to cast ballots. Robust authentication has proven to be a complex problem because, among other reasons, databases contain errors and are corruptible through the human element. The fact that there are inevitably errors in databases means that human

judgments are still required. A database sometimes simply provides the wrong answer more quickly.

A trade off in privacy exists in the legal requirement of voter registration to participate in publicly held elections. Voter registration has been championed as a means of discouraging repeat voting and the importation of voters from other jurisdictions to cast votes in local and some state elections. Each state is responsible for administering voter registration within its boundaries. Today voter registration forms may include requests for name, current and previous address, home and work telephone numbers, birthplace, social security number, birth date, race, gender, and party affiliation.

HAVA requires that voter registrants submit proof of identity by providing a state-issued identity document or the last four digits of their social security number. Non-citizens may be deported for voting in local, state, or federal elections

In any case, human judgment is used in the gatekeeper function of poll workers to determine who may vote. Unfortunately, the voters who are demographically dissimilar from poll workers often find hurdles to voting. For example in the State of Florida voters erroneously included on a list of felons, who are prevented by state law to vote, were predominately minority. Some poll workers were able to recognize the errors on the list and allowed voters to vote, while others did not allow these individuals to vote. Poll workers should not be gatekeepers to the ballot box, but the focus should be on facilitating participation in the election process. (Other suggestions in this document on provisional voting, if followed, would remove poll workers from the goal of gate-keeper.)

4. Good Voting Systems Require Good Design Standards

Technological systems can and do embed values; this is best acknowledged through design standards and review processes. Technology is rarely neutral. Biases can be direct (disenfranchising

those with special needs) or persuasive (making one vote easier than another to cast). Such biases can be unintentional; for example, the result of a neutral design simplification can create a persuasive bias when a particular vote is made more difficult to cast by creating an unnecessarily complex ballot.

4.1 There is no single voting interface that can meet everyone's needs.

American voters have a diverse range of needs and preferences. Different localities may seek to place emphasis on different features of the interface, respecting the priorities of the local population and culture.

Within a jurisdiction, there is no need for everyone to use the same interface as long as no one is deprived his or her basic rights of access. The interface to voting technology should not be standardized, but rather a community should seek to ensure that everyone could cast his or her ballot comfortably, conveniently and with confidence.

4.2 An untrained voter should be able to know when voting equipment fails.

Just as testing and auditing help give the voter a degree of confidence about the security of the equipment and the robustness of the process, the user of a voting system should be able to know when any critical aspect of that system fails. Poll worker intervention or system redundancy improve detection and recovery in the case of failure. Since the officials and vendors cannot and should not monitor every single vote, having this added degree of auditing is necessary. Voters are the final audit. A controversy such as in Florida in 2000 could not have occurred if each voter knew at the time of the vote that they had marked the punch card correctly for the candidate and for their ballot to be read by the tallying machines.

4.3 Access is critical: not to a specific, single technology, but to the ability to vote in a fashion that provides full civil rights.

The greatest privacy benefit of electronic voting systems accrue to those who have physical disabilities, are language minorities, and those with literacy difficulty. Accessible technologies offer for the first time for many of these voters privacy and independence in voting in public elections. Audio marking systems, or OCRs with tactile ballots can also be used with visually impaired, and those with literacy difficulty. DREs and appropriate paper ballots can be used by language minorities.

Note that everyone is not best served by the same interface; for example, when a substantial portion of the population is unfamiliar with the use of screen-based interfaces such as those found on Automatic Teller Machines (ATMs) then relying on that model may alienate or confuse those voters.

4.4 Even with full auditing of each vote, rigorous testing for security, usability and reliability remains critical.

Security, reliability and usability are necessary for any successful voting system. Security is a measure of confidence against malicious attack, while reliability is a degree of confidence that the system will function as intended. Usability is a metric of whether the voter can cast the ballot her or she intends. None of these can ever absolute, but comparative measures are possible: is one system more or less reliable than the other?

Testing must occur at three distinct junctures. First, the prototype model must be rigorously inspected and analyzed to make sure that it meets the original design specifications and standards and will function as intended. Second, the machines delivered to the polling places must be determined to be the same machines requisitioned, and any new software or features do not violate the original standards. Finally, the

assembled and installed machines must be certified to be properly set up and calibrated, with all the functions operating as predicted.

Beyond the laboratory and polling place settings, these systems can be tested in the public by the very voters who will be using them. Colleges and high schools can use the machines for student elections, or marketing firms can deploy them in malls to gather consumer opinions. This has the combined effect of raising public awareness and familiarity with the new technology and subjecting machines to real-world stress conditions.

Testing is required in addition to voter-based outcome auditing and is not a substitute for such first person auditing. Testing can certify that the machine will function and will have usable interfaces. Section 6 of this document addresses auditing in more detail.

5. Transparency Builds Public Trust and Supports Legitimate Elections

Privacy and transparency are necessary components to any democracy; without both the system fails. Independent review is an important beginning, but true transparency demands testing and verification for accuracy and integrity, audit, and open standards. To make the assurance to a voter that his or her individual vote is valid and private requires more than the assurance of technologists and voting technology vendors. Voting technology must be transparent in means and methods. Voters should be able to easily access public meeting records, system evaluation tests, performance information from other jurisdictions and other relevant information on the voting technology to which they entrust their votes on Election Day. Voters with disabilities or special needs ideally should have private, accurate votes. The current system of paperless DRE voting technology fails in that privacy means both that a vote is confidential and that the voter is assured of this confidentiality.

A process that is seen by many will have a greater degree of legitimacy than a closed process. Open code enables true transparency in digital processes.

5.1 If underlying mechanics or software are not in the public domain, they must at least be available for inspection by the larger security community.

The greater the number of qualified experts examining a system, the greater the chance that a security flaw can be discovered. Given that determined attackers will be searching for weaknesses as well, if is in the public's interest for election officials to discover and fix security flaws first. Full public examination of the software code underlying digital voting technologies is no guarantee of perfect security—this is impossible—but allowing the public at large to scour the code increases the likelihood that weaknesses in the code will be discovered. If the source code of the software is protected by intellectual property laws, granting access to the code is an added difficulty. Restrictive intellectual property practices which prevent code review are unacceptable in the realm of voting. For this reason, among others, open software code is ideal for software used in any equipment that reads, counts, or tallies votes. Exposure of the underlying code serves as a further incentive for the vendors to write good code. Nondisclosure agreements have no role in realm of voting.

5.2 All security issues should be fully disclosed, although allowing vendors a limited, fixed time between notification and public disclosure could foster more public trust.

Hiding security flaws has never been a robust security strategy. Security flaws should be revealed and fixed. The timing of public disclosure has been an issue of active debate in the computer security field. A short delay between discovery and exposure can encourage the vendor to fix the problem as quickly as possible, but too short a delay might not give the vendor enough time. Publication of a security

flaw before widespread implementation of its solution can open the door to exploitation of the security flaw. It is ultimately the vendor's responsibility to fix security issues. As mentioned previously, if a vendor fails to respond in a timely manner contracts should not prevent officials from obtaining assistance elsewhere.

5.3 The voting technology acquisition process should be open for public scrutiny from constituents.

Just as the underlying technology should be open for criticism, so too should the process by which the technology is selected be open and public. One fear is regulatory capture, where the government officials grow too close with the voting systems vendors as their primary source of information. Officials should be forced to justify the decisions they make with respect to selecting certain technologies and rejecting others, including the initial decision to change the voting process from its current manifestation. Furthermore, openness of purchase allows individual constituencies of the decision maker to have their say, and the officials to show that they have taken these views under consideration.

5.4 The voting technology acquisition process should be open to allow jurisdictions to learn from each other. Records of difficulties should be made available to all election officials.

There is a strong tradition in information technology of "user communities" where owners and adopters of technology share information, both to help in their own experiences and to encourage common vendors to play fairly. Assessing the needs of a community and purchasing a voting machine is not a common decision for local elections officials, so it is hard for them to gain experience and acquire reputation information. All jurisdictions should try to avoid reinventing the wheel, and should learn from each other. This can prevent bad decisions and vendor deception.

6. Election Systems Must Have Built-In Auditing Capability.

A certified election asserts that the vote that was counted is the same vote that was cast by the voter. As such, if there is any question about the execution of an election, the results must be subject to critical examination. This auditing process needs to be informed by the underlying technology, but all audits have must certain properties. An audit includes a recount of the ballots, but can also involve an examination of the systems used, the process of the election and the possession and treatment of the ballots. A DRE system with no physical record of individual votes cannot meet these criteria.

6.1 The reconciliation process must be clear, precise, authoritative and binding.

The audit process derives its authority by being designed and subject to scrutiny before the election. It must be designed to confer legitimacy on the results, and should be acknowledged by all parties. The general public must understand what is going on, and exactly what will be ascertained by an audit. This includes an awareness of what will and will not be verified by the audit.

A binding reconciliation process should not be open to direct challenges. That is, concerned parties should only be able to argue that it was not executed properly, not that the auditing plan itself was flawed during an audit. The rules of engagement must be determined before the conflict over outcome. Clarity, precision, clear authority, and binding reconciliation in the process which answers questions about an election gives credibility to those answers.

6.2 The cast ballot must follow a "chain of custody" from the moment it is cast to the moment the vote is entered into the final official tally.

The chain of custody must be subject to audit and oversight at each step regardless of technology. The nature of the audit and oversight may be specified based on the technology.

Throughout this process, no one actor should be able to secretly destroy or alter ballots. Partisan competition and dual-party monitoring can be used as safeguards. Each ballot must be accounted for. It is important to also respect the anonymous nature of each ballot. Each voting jurisdiction must make adequate preparations for an audit for each election, so adequate numbers of officials, observers and law enforcement are available if needed. The myriad issues that can arise in the auditing process should be addressed by election officials' contingency plans.

6.3 If some metric of voting irregularity is exceeded in a given jurisdiction, a court-supervised manual recount should be required.

Many voting irregularities can be traced back to flaws in the voting systems. Any recount that is concerned with error introduced by the voting systems themselves should deal with the most auditable mechanism, ideally voter-verified paper ballots. Triggering an automatic audit at a certain threshold does not preclude audits from occurring at other times, but saves the trouble of argument in an obviously close or questionable elections. Such audits evaluate the vote- casting and counting systems as well as the outcome. For example, California requires a 1% randomly selected hand recount as a systematic check on accuracy.

6.4 Auditing should not be implemented by a vendor affiliated with the original system.

In the event that the election officials turn to the private sector to aid in the auditing process, the standard industry practice must be used for securing and independent, third-party system. The purpose is to examine the entire system, not just the votes, so having an outsider view the technology can help guarantee less opportunity and motivation for bias or even malevolence. Systems in which the

technology and code are open to examination make this process more straightforward.

6.5 Equipment testing does not displace the need for outcome auditing.

Testing is necessary but not sufficient for a well-run election. Testing is never perfect, as it can overlook certain factors or interactions that may be easier to detect in hindsight. Systems interact with each other in unpredictable ways, often impossible to detect in a reasonable battery of tests.

It is also very difficult to predict the human element, be it simple mistakes or partisan manipulation, so usability testing is critical regardless of the system. Every configuration should be tested as appropriate.

Outcome auditing can confirm the validity of testing for future elections although; however, it is a complement to and not a substitute for such testing. Outcome auditing cannot test for usability; testing before the vote cannot verify accuracy of final tally. Paper ballots are independent non-aggregated artifacts that can provide outcome auditing, yet paper ballots also require usability testing.