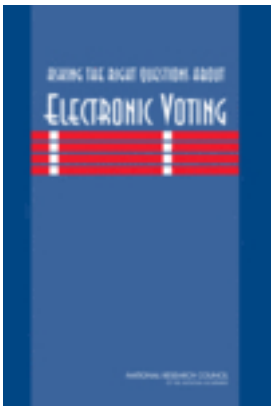

Asking the Right Questions About Electronic Voting

Richard Celeste, Dick Thornburgh, and Herbert Lin, Editors, Committee on a Framework for Understanding Electronic Voting, National Research Council

ISBN: 0-309-65394-0, 162 pages, 6x9, (2005)

ASKING THE RIGHT QUESTIONS ABOUT ELECTRONIC VOTING

Richard Celeste, Dick Thornburgh, and Herbert Lin, editors

Committee on a Framework for Understanding Electronic Voting
Computer Science and Telecommunications Board
Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by the National Science Foundation (NSF) under Award Number IIS-0436133. However, in accordance with National Research Council policy, the NSF did not review this report before publication, and the opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the NSF.

International Standard Book Number 0-309-10024-0

This report is available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu.

Printed in the United States of America

Suggested citation: National Research Council, Asking the Right Questions About Electronic Voting, Computer Science and Telecommunications Board, The National Academies Press, Washington, D.C., 2006.

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Wm. A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Wm. A. Wulf are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON A FRAMEWORK FOR UNDERSTANDING ELECTRONIC VOTING

DICK THORNBURGH, Kirkpatrick & Lockhart Nicholson Graham, LLP, *Co-Chair*
RICHARD CELESTE, President, Colorado College, *Co-Chair*
R. MICHAEL ALVAREZ, California Institute of Technology
THOMAS SHERIDAN, Massachusetts Institute of Technology (retired)
JOSEPH A. SMIALOWSKI, Freddie Mac
ANTHONY STEVENS, State of New Hampshire
PETER WEINBERGER, Google Inc.

HERBERT S. LIN, Senior Scientist and Study Director
KRISTEN BATCH, Research Associate
TED SCHMITT, Consultant
BRANDYE WILLIAMS, Staff Assistant

Preface

The public debate about electronic voting is characterized by a great deal of emotion and rhetoric. Today, the major protagonists seem to be election officials who hope that electronic voting systems can improve their ability to conduct and administer elections more efficiently and computer scientists, information technologists, and election activists who are skeptical about the viability of using such systems (electronic voting skeptics) for functions critical to the operation of a democracy. Policy makers are thus caught in the midst of a controversy with both political and technological overtones.

However, as is often the case, the public debate captures only some of the important elements of the issue—most notably, security. As a variety of social scientists have argued and demonstrated, there are a number of other issues relevant today that have a dramatic and significant impact on the conduct of elections.

To understand the larger debate and gain a fuller appreciation of its complexity (that is, accounting for security as well as other important dimensions of the issue), the National Research Council (NRC) began with an internally funded meeting on the subject on July 13-14, 2004. The July 2004 meeting was well attended by a variety of individuals with diverse points of view and expertise. These individuals (listed in Appendix C) included computer scientists and information technologists with expertise in security, user interface design, and large-scale system deployment; political scientists; election officials; civil rights advocates for

minorities and people with disabilities; and election systems vendors. This meeting was designed to air issues and to raise important questions, rather than to come to consensus on any particular topic.

After this meeting, the NRC received support from the National Science Foundation to take a first step in a more thorough examination of this subject by developing a reasoned understanding about it. In the present case, the NRC decided that the approach of focusing on questions and raising issues would be a good way to develop such an understanding. To support the work of the cognizant committee, known as the NRC Committee on a Framework for Understanding Electronic Voting, two open sessions were held in which the committee heard from various participants in the public debate over electronic voting; Appendix C lists the briefers at these open sessions. In addition, the committee issued an Internet call for white papers on electronic voting; the papers received are listed in Appendix C and can be found online in their entirety at http://www7.nationalacademies.org/cstb/project_evoting.html#papers. The committee was able to draw on a rich base of information and expertise to inform its deliberations, including the proceedings of the July 2004 meeting.

PURPOSE AND SCOPE OF THIS REPORT

The primary intent of this report is to describe some of the important questions and issues that election officials, policy makers, and informed citizens should ask about the use of computers and information technology in the entire electoral process, thus focusing the debate on technical and policy issues that need resolving. The material in this report is not intended to turn election officials into computer scientists, but rather to help election officials to better understand the perspectives of electronic voting skeptics who have been active in the debate, to help them understand what the electronic voting skeptics are saying and why they are saying it, and to appreciate some of the questions about electronic voting technologies that worry many technologists. The committee also hopes that this report will inform in the reverse direction as well, helping electronic voting skeptics to better understand election officials, the pressures that drive them, and the demands they face from various quarters.

In the months preceding the start of this project, a number of participants and advocates in the public debate over electronic voting took issue with this focus on questions and the timing of the effort. Some asserted that the debate over questions had already been settled and that what was needed now was authoritative answers. Others asserted that by the time this report was released, the states would already have made commitments to purchases of electronic voting systems, and that the only meaningful advice to be given would be to throw out those systems and start

over again. Indeed, some of these advocates thought that this would be a good idea.

From the committee's perspective, the prior groundbreaking work undertaken by many of these advocates helped enormously to inform its effort. Nevertheless, the committee believes that a "ground up" understanding of what the issues are—developed by individuals who for the most part have not taken a stand on them—has analytical and probative value. As for the timing, the committee believes that the electronic voting issue will be with us for many years into the future because of upgrades, changes in the vendor base, and rapid change in the underlying technology base.

The committee does agree that a consensus on authoritative answers should be developed. Had this project not been constrained by time and funding, it would have been the committee's desire to seek such a consensus. It is the NRC's and the committee's hope that this report will nonetheless be a step in that direction.

Finally, the committee cautions that the questions it poses in this report should not in themselves be interpreted as a vote of confidence or of no confidence in electronic voting systems. As with the adaptation of technology for a variety of different purposes and applications, such a vote depends on the maturity level of the technologies involved and how they are used—and the questions posed by the committee are intended to help election officials gain more insight into these matters.

PERSONAL NOTE FROM THE CHAIRS

Those thoughtful about the nature of democracy realize that democracy is always an exercise in managing and dealing with risk, a never-finished piece of business. That is, in the course of governing, some things will always go wrong, and action will be needed to set things right—and some things about elections, as a part of democracy, are no exception.

As former participants in public life, we have both won and lost elections and obviously care deeply about the extent to which elections can be said to reflect the will of the people. In addition, we both know of instances in which problems in a particular election may have affected the outcome and certainly did affect the final vote tallies. But as distressing as such errors or problems are, we remain confident in the strength of democracy to take steps to ensure that these errors or problems do not occur again, and to move on.

New information technologies have profoundly changed the sectors of society where information is involved, and there is no reason to expect that elections will not be subject to the same kinds of influences as other areas of society and national life where accurate and reliable information

gathering is at a premium. At the same time, and as would be true for the early stages in the adoption of new technologies for any application, there are many currently unresolved issues related to changes in the voting environment.

It is for this reason that both of us joined this project—to understand the ramifications of electronic voting for the conduct of elections. We believe that those ramifications are indeed complex, but not so complex as to defy rational and systematic investigation. We believe that the issues associated with electronic voting are not partisan issues, not systematically associated with the interests of either Republicans or Democrats. We believe that the questions for election officials developed in this report represent a good start on such an investigation. We believe that the voting public should be involved in asking these same questions—and paying heed to the answers they receive.

We extend the committee's appreciation to those who took the trouble to contribute to the committee's deliberations in person and in writing. Without them, this report would simply have been a distillation of our personal prejudices and intuitions. We appreciate the wisdom, insights, and tutelage of our fellow committee members. And we offer special thanks to the National Research Council for providing a stellar study director, Herbert Lin, whose tenacity and commitment made a world of difference to our project.

Richard Celeste, *Co-chair*
Dick Thornburgh, *Co-chair*
Committee on a Framework for
Understanding Electronic Voting

Acknowledgment of Reviewers

This report was reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's (NRC's) Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

Stephen Ansolabehere, Massachusetts Institute of Technology,
Elwyn Berlekamp, University of California, Berkeley,
Henry Brady, University of California, Berkeley,
David Jefferson, Lawrence Livermore National Laboratory,
Butler Lampson, Microsoft, Inc.,
Neil McClure, Hart Intercivic,
J. Brad Mooney, Independent consultant,
Sharon Priest, Downtown Partnership, Inc. of Little Rock, Arkansas,
Scott Robertson, Drexel University, and
Fred Schneider, Cornell University.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the con-

clusions or recommendations nor did they see the final draft of the report before its release. The review of this report was overseen by Lewis Branscomb of Harvard University. Appointed by the NRC, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Contents

Executive Summary

BACKGROUND

Electronic voting is controversial today. Many election officials look to electronic voting systems as a means for improving their ability to conduct and administer elections more efficiently. At the same time, many information technologists and activists have raised important concerns regarding the security of such systems. Social scientists have studied election issues for many years and have identified a host of issues that have significant impact on the conduct of elections. Policy makers are caught in the midst of a controversy with both political and technological overtones.

Given this backdrop, the National Research Council (NRC) sought to examine this issue from the ground up—that is, from a broader perspective than simply addressing the most salient points in the public debate. A first meaningful step in such an examination should be the articulation of important questions and issues that election officials, policy makers, and informed citizens should ask concerning the use of computers and information technology (IT) in the electoral process. In addition, the NRC's Committee on a Framework for Understanding Electronic Voting reached a number of conclusions that help clarify the nature of the debate over electronic voting systems and provide a framework for putting these questions into perspective.

FINDINGS

The committee found that **electronic voting systems offer potential for voting and election management that is an improvement over what has thus far been available. However, the realization of this potential requires a commitment to this path by the nation, the states, and local jurisdictions that is not yet evident.** Taking this path will require, among other things, research, funding, educational efforts, and new standards and testing processes.

A second important point, obvious yet often overlooked in the public debate, is that the introduction of electronic voting systems is intended to make elections better. That is, **the desirability of electronic voting systems should be judged on the basis of whether their use will significantly improve the process of election administration.** When new voting systems offer an opportunity to significantly improve at reasonable cost the process of election administration in multiple dimensions over what it is today—for example, to make election administration more efficient, less costly, more trustworthy and secure, and so on—it makes sense to consider their deployment. But merely marginal improvements are rarely if ever worth the cost of the disruption associated with introducing new systems.

Third, **judgments about the ultimate desirability and feasibility of electronic voting systems should not be limited to the features and flaws of the systems demonstrated to date.** Today's debate over electronic voting systems has been framed largely by examination of the electronic voting products of today. But technologies improve over time, and it is thus inappropriate to make strong generalizations about the systems of tomorrow based on inspection of the systems of today. At the same time, there are some technical realities that are exceedingly likely to persist over the long run. Conclusions based on such realities do have a staying power that conclusions based on today's state of technology do not.

Fourth, **trusted election processes should be regarded as the gold standard of election administration,** where a trusted election process is one that works, can be shown to have worked after the election has been held, can be shown to have not been manipulated and to have not led to a large number of mistaken or lost votes, and can be shown to reflect the intent of the voters. Trusted election processes increase the likelihood that elections will be regarded as fair, even by the losing side and even in a partisan political environment.

Fifth, the committee believes that many parties have made important contributions to the public debate over electronic voting:

- **Electronic voting skeptics have raised important questions about the security of electronic voting systems that should not be discouraged**

or suppressed. Electronic voting systems, like all complex systems, are fallible and susceptible to deliberate or accidental compromise, and some kind of backup against the possibility of fraud or malfunction should be available if and when allegations of such occurrences arise. The paper trail may be a mechanism that can serve this function, but whether it is the only or most appropriate such mechanism has yet to be determined.

- **Political scientists who have studied elections for many years have identified data whose collection would enable the public to judge the accuracy and usability of voting systems in use and the accuracy and reliability of the voter registration systems used by states, counties, and municipalities.** Independent observers need relevant and reliable data in order to judge the adequacy of the systems in use, and election officials should be encouraged to acquire such data and to make it publicly available.
- **Legislators in many states have publicly aired many important issues related to electronic voting.** In so doing, they have placed a considerable amount of useful information on the public record, and they have successfully balanced a variety of concerns in some of their legislative efforts.

At the same time, election officials are properly and appropriately concerned about many aspects of election administration, and they must balance a variety of considerations—including security, speed and accuracy of reporting election results, usability, affordability, voter turnout, and compliance with federal, state, and local election laws. It is entirely reasonable and understandable that they take an operational perspective, as might be expressed in the question, Will a particular electronic voting system help to significantly improve election administration and management with respect to all of those considerations? If they can in good conscience answer this question in the affirmative, acquisition of such a system is justifiable.

SETTING THE STAGE

Three threads combine to set the stage for the bulk of the work of the Committee on a Framework for Understanding Electronic Voting. The first is the electoral process, which is complex and highly decentralized. The Constitution of the United States has given to the states the rights and responsibilities for conducting elections for more than 200 years, and 9,500 jurisdictions within the 50 states and the District of Columbia have developed a wide variety of election processes. Election administration in the United States at all levels costs an estimated $1 billion per year.

The second thread is the need for public confidence in democratic

elections. A sine qua non for the legitimacy of democratic government is elections that are perceived to be fair by both winners and losers. Indeed, it is often said that the main purpose of election fairness is to convince the loser and his or her supporters that the election was lost fair and square—winners rarely complain about the fairness of an election.

Certain aspects of the political environment today make it more difficult for certain elections to be perceived as fair. Bitter political campaigns and an evenly divided electorate are breeding grounds for postelection rancor, on the theory that even a small amount of deliberate fraud or accident or mishap or improperly followed procedure might have tipped the election the other way. Elected public officials such as governors and secretaries of state are usually associated with one party or another, and decisions that favor their own parties are often seen as partisan. The cost of some elections (primaries, in particular) exceeds $100 per vote received and has led some analysts to wonder if this high cost raises the incentives to cheat in an election. And, vendors of electronic voting systems have not always been seen as politically neutral.

The third thread is voting technologies (i.e., technologies for casting and counting ballots). A variety of electronic voting systems have been proposed to improve election administration and to reduce the problems and errors associated with nonelectronic systems. In the public debate, the term "electronic voting system" has been used to refer to a computer-based voting station located in the polling place with which citizens interact directly to cast their ballots. (A voting station refers to a single unit, usually used in the polling place. An electronic voting system refers to the generic hardware and software involved.) But computer-based systems can and do support the electoral process in at least three other important ways: voter registration lists are maintained on computer-based databases, and vote tabulation and ballot definition are election-related tasks conducted on computer-based administrative systems.

Electronic voting is appealing to election officials because it promises significant reductions in the logistical burdens of election administration. In addition, election officials believe that the level of expertise required to commit election fraud is much greater than when nonelectronic systems are used. If greater expertise is required, fewer people will be capable of perpetrating election fraud. From a usability perspective, electronic voting systems offer programmable user interfaces that provide a high degree of customization to voter needs or preferences (e.g., voters more comfortable in languages other than English, or voters with disabilities).

For these reasons, it is likely that over the long run, electronic voting systems will supplant nonelectronic voting systems. But acknowledging this trend over the long run does not mean that acquisition of such systems should happen before important questions about these systems are resolved. It is in this spirit that the questions posed in this report are offered.

INFORMATION TECHNOLOGY FOR VOTER REGISTRATION

Voter registration is affected by information technology, and yet the subject receives little attention in the public debate. Voter registration is the gatekeeping process that seeks to ensure that only those eligible to vote are indeed allowed to vote when they arrive at the polls to cast their votes.

Voter registration is a complex process, and maintaining voter registration databases is highly dependent on information technology. Two primary technology-related tasks for voter registrars are to keep ineligible individuals off the registration lists and to make sure that eligible ones who are on the lists stay on the lists. These tasks arise because individuals identified as eligible voters may lose their eligibility to vote for a number of reasons (e.g., death) or their eligibility to vote in particular electoral contests (e.g., because of a change of address).

Because lists of registered voters contain millions of entries, the removal of ineligible or improperly registered names from a voter registration list (purging) must be at least partially automated. That is, a computer is required to compare a large volume of information received from other sources (e.g., departments of vital statistics for death notices, law enforcement or corrections agencies for felony convictions, departments of tax collection or motor vehicles for recent addresses) against its own database of eligible voters to determine if a given individual continues to be eligible and properly registered.

Any purging process is prone to two types of error. Some properly registered voters will be incorrectly identified as ineligible and thus improperly purged. Also, some ineligible voters will not be identified as such and thus will remain on the list. It is a fundamental reality that the rate of these errors cannot be driven to zero simultaneously. The more demanding the criteria for a match, the fewer the matches that will be made. Conversely, the less demanding the criteria, the greater the number of matches that will be made. The choice of criteria for determining similarity is thus an important policy decision, even though it looks like a purely technical decision.

Questions About Voter Registration Systems

4-1. Are the relative priorities of election officials in the purging of voter registration databases acceptable (placing greater importance on preventing the improper purging of eligible voters or on purging all possible ineligible voters)?

4-2. What standards of accuracy should govern voter registration databases?

4-3. How well do voter registration databases perform?

4-4. What is the impact on voter registration database maintenance of inaccuracies in secondary databases?
4-5. Will individuals purged from voter registration lists be notified in enough time so that they can correct any errors made, and will they be provided with an easy and convenient process for correcting mistakes or making appeals?
4-6. How can the public have confidence that software applications for voter registration are functioning appropriately?
4-7. How are privacy issues handled in a voter registration database?
4-8. How can technology be used to mitigate negative aspects of a voter's experience on Election Day?
4-9. How should voter registration systems connect to electronic voting systems, if at all?

INFORMATION TECHNOLOGY FOR VOTING

The main technology discussion of this report addresses two areas of particular significance: security and usability.

Security

Security issues in voting are among the most complex that arise in the development of secure systems for any application. Systems to manage financial transactions, for example, must also be highly secure, and much of the experience and knowledge needed to develop financial systems is directly applicable to electronic voting systems. But one key difference between financial and voting applications is the need to protect a voter's right to a secret ballot. Developing an audit procedure (and the technology to support audits) is enormously more difficult when the transactions of an individual must not be traceable to that individual.

A second important point is that election systems must declare a winner even when the margin of victory is minuscule. That is, when the vote is close, a very small number of votes can sway the election one way or another. Thus, in closely contested races, a person intent on committing election fraud must manipulate only a small number of votes in order to obtain the desired outcome—and small manipulations are intrinsically more difficult to detect than large ones are.

Much of the public debate over electronic voting systems has been driven by computer scientists, for whom security is a particularly elusive goal. It is elusive because no reasonable amount of system testing can prove that a system is free of security vulnerabilities, and because would-be attackers are motivated to continuously explore a system for such vulnerabilities. When approaching any computer security problem, the

computer scientist's perspective can be summarized as a worst-case perspective—if a vulnerability cannot be ruled out, it is necessarily of concern. Computer scientists are also concerned because the use of computers for voting purposes enables small numbers of individuals to practice fraud on a much larger scale than has been the case with nonelectronic systems.

The perspective of the election officials is quite different. Election officials are responsible for the safety and security of an election, and as a rule, they accept that the burden of assurance properly rests on their shoulders. But even with traditional voting systems, vulnerabilities to the integrity of an election abound. The administrator is concerned with the integrity of the election from the point of voter registration to the moment of winner certification. Within that entire process, there are many opportunities for something to go wrong—both deliberately and accidentally—that can potentially affect election outcomes. Election officials do not have the resources to deal with all problems or vulnerabilities, and they necessarily leave some unaddressed. Within the constraints of their limited resources, they tend to address problems as they become known (that is, as they are shown to affect actual elections), and so the election official's perspective is one of seeking incremental improvements in existing systems or to existing procedures.

Consider how these different perspectives play out in the consideration of election fraud. Election fraud, or the appearance of fraud or impropriety, can undermine public confidence in elections. But whereas computer scientists will presume that a vulnerability is significant until shown otherwise, election officials are willing to presume that the integrity of an election has not been breached until some evidence is produced to the contrary. This difference in perspective largely accounts for the tendency of some election officials to blame electronic voting skeptics for scaring the public about security issues, and for the tendency of some computer scientists to say that election officials have their heads in the sand.

Questions About Security

4-10. To what extent and in what ways has a realistic risk analysis been part of the acquisition process?
4-11. How adversarial has the security assessment process been?
4-12. How has the system's ability to protect ballot secrecy been assessed?
4-13. How is the security of voting stations maintained to ensure that no difficult-to-detect tampering can occur between receipt from the vendor and use in the election?

4-14. What steps have been taken (either technically or procedurally) to limit the damage an attacker might be able to inflict?
4-15. How can election officials be sure that the voting systems in use on Election Day are in fact running the software that was qualified/certified?
4-16. What information must be collected on Election Day (and in what formats) to ensure that subsequent audits, recounts, or forensic analysis can take place if they are necessary?
4-17. How are anomalous incidents with voting systems reported and documented?
4-18. What is the role of parallel testing?
4-19. What physical security provisions will be put into place at polling places after the voting stations have been delivered but before the polls open?
4-20. What physical security provisions will be put into place immediately before the polls open and immediately after the polls close?
4-21. What physical security provisions will be put into place at polling places while the polls are open?
4-22. How are the results from polling stations communicated to the central tabulation authority?
4-23. How does the central tabulation authority aggregate vote totals?
4-24. What physical security provisions will be put into place at the central tabulation authority?
4-25. What roles can postelection auditing and investigation routinely play to increase the likelihood that fraud or other problems will be detected?

Usability and Human Factors Engineering

All voting systems face the usability problems of accurately capturing the voter's intent in casting a ballot and being easy for voters to use, and there are numerous challenges with regard to the behavior of human users. Indeed, the importance of usability was highlighted by the infamous butterfly ballot in the 2000 presidential election in Palm Beach County, Florida, which allegedly confused many voters into casting a ballot that was contrary to their intent.

Electronic voting promises many advantages from a usability standpoint, but there is no single best way to capture voter intent. Consequently, different vendors and different election officials can legitimately and ethically make different decisions about how best to present information to the voter and how best to capture the voter's vote.

For much of the past, usability issues in ballot marking systems were limited to a consideration of physical accessibility of the voting booth to the voter and translation of the ballot into other languages for non-English-speaking voters. But as the 2000 election demonstrated so clearly, there is much more to usability than access. Indeed, in a voting context, usability includes human factors (perceptual, cognitive, and motor capabilities); background (language, education, culture, past experiences); complexity and extent of the task (arrival, departure, waiting in line, asking for help, etc.); situational and environmental contexts, such as the physical situation (adequate lighting, electricity, heating, etc.) and the social situation (crowds and time limits); sociological issues (privacy, confidence in technology, and equity issues); psychological factors (workload, attention, situation awareness, and distraction) that constrain people's actions; and differences between designers and users in their perceptions of what a system should do. Participatory design, in combination with rapid prototyping, is a widely used method for user-centered development of new technology systems, especially where usability concerns are important (e.g., consumer products that compete in the mass marketplace and safety-critical systems).

Ballot marking systems pose a particularly difficult usability challenge. Ballot marking systems must be highly usable by the broad public. A citizen in the voting booth facing an electronic voting system may not feel comfortable with information technology, may not be literate (with everyday reading and writing, to say nothing of being computer literate), may not speak English, may have physical disabilities that interfere with the actions needed to cast a vote, and is generally alone in the booth (and thus may not be able to call for help from friends or colleagues). Perhaps most important, very few voters have a chance to vote more than once or twice a year and thus have little opportunity to develop experience or familiarity with the system.

Questions About Usability and Human Factors

4-26. How does a voter receive feedback after he or she has taken an action to cast a vote?
4-27. How is an electronic voting system engineered to avoid error or confusion?
4-28. What accommodations have been made to address the special concerns and needs of people with disabilities?
4-29. What accommodations have been made to address the needs of non-English speakers, voters with low literacy skills, and citizens from various cultural, ethnic, and racial groups?

4-30. How and to what extent have concerns about the needs of these parties been integrated into the design of the system from the start?
4-31. What are the ballot definition capabilities offered to jurisdictions?
4-32. How is provisional balloting managed?
4-33. What is the range of the subjects used in testing usability?
4-34. What is the error rate in capturing votes of any given system? How is that error rate determined?
4-35. What are the submetrics of usability that are applied to evaluate and compare systems?
4-36. To what extent, if any, do problems with usability systematically affect one party or another, or one type of candidate or another?
4-37. How is feedback from actual usage incorporated into upgrades to currently deployed systems?
4-38. How does usability testing incorporate the possibility that different jurisdictions may create ballots that are very different from one another?
4-39. Who should conduct usability testing on specific ballots?
4-40. How long does it take a first-time user to become familiar enough with the system to use it reliably and with confidence?
4-41. What kinds of educational materials should be prepared and distributed in advance?
4-42. To what extent are practice systems available for use before and on Election Day?
4-43. What voter assistance can the voting station itself provide to users?

Reconciling Security and Usability

Election officials often believe that security and usability are necessarily traded off against one another. However, in the design of electronic voting systems, the trade-off between security and usability is not necessarily so stark. That is, there is no a priori reason that a system designed to be highly secure against fraud cannot also be highly usable and "friendly" to a voter, even if these goals may be in conflict at some point after attempts at "better design" or "better engineering" have been exhausted.

THE LIFE CYCLE FOR INFORMATION TECHNOLOGY SYSTEMS

The initial decision to procure an information technology system is only one dimension of the life cycle of that system, and the acquisition of information technology has many other dimensions. The life cycle of a system begins with its initial purchase or acquisition—that is, when the system is first delivered. Concurrently, people must be trained to use,

operate, and maintain the system. Problems in operation are inevitably discovered, ranging from small software bugs to major design flaws—and many of these problems must be fixed. Fixing a problem involves the development of a putative fix itself and then testing the fix to determine that the problem is resolved and that no other problems are introduced. Then the problem fix must be deployed to the entire installed base of systems. In addition, new capabilities are often desired by the user, and a vendor may develop upgrades to accommodate those needs; upgrades must go through the same process of development, testing, certification, and deployment as do problem fixes.

The initial procurement cost of any information technology system is generally only a fraction of its total life-cycle cost, which includes additional costs associated with operations, maintenance, upgrades, and training. (Put differently, within a few years of initial purchase, many states have found that other nonprocurement expenditures exceed the initial purchase cost.) In addition, costs beyond initial procurement can increase dramatically in later years if vendor support for the purchased configuration is not available. Over some period of time, it is likely that this will be the case, either because the vendor will have made available upgrades to the initially deployed system and no longer supports that system, or in less common instances because the vendor has simply gone out of business.

Given that elections happen relatively infrequently, continuity of the election process is an important requirement. Purchasers of electronic voting systems (that is, states or local election jurisdictions) must have assurances that a vendor will be able to support those systems for an extended period of time.

Questions About the Life Cycle of Electronic Voting Systems

5-1. What is the life-cycle cost of any particular electronic voting system?
5-2. What assurances can a vendor offer with respect to long-term support?
5-3. What are alternatives to purchasing complete integrated voting systems?
5-4. How difficult will it be to change vendors if the original vendor becomes unresponsive or too expensive?
5-5. What logistical and administrative issues arise regarding the physical management of a voting system?

POLL WORKER TRAINING

Poll workers play an essential role in the electoral process today. But in the context of electronic voting systems, the range of things a poll worker might be responsible for doing is arguably even larger than when

nonelectronic systems are used. This is not to say that every poll worker will necessarily experience a wider range—only that he or she must be trained to handle a larger number of contingencies. In general, poll workers must know how to use the systems at least as well as any voter would need to know, and they must know still more than that, because they will be the first line of assistance for voters who are confused about how the system works. Poll workers must know enough about the system in use to be able to recognize a problem that arises at a voting station, and then to take action to correct the problem.

Questions About Poll Worker Training

5-6. What is the nature and extent of the training required to make poll workers sufficiently knowledgeable about an electronic voting system?
5-7. How will election officials know that a poll worker has been adequately trained?
5-8. How will poll workers get help when unanticipated questions or issues arise?
5-9. What is the nature of the help mechanism(s) provided by the vendor?
5-10. What consequences flow from any vendor inability to provide adequate problem resolution on Election Day?
5-11. How can local election officials attract and ensure an adequate base of volunteers who can cope with the challenges of new electronic voting systems?

DATA

Data are lacking on many aspects of the electoral process that are needed to make improvements or to conduct audits. With high-quality, consistent data in hand, a great deal can be learned about the workings of voting machines, voter registration systems, and reforms in different states that would inform the election administration process. Also, because voting is a decentralized affair, data must be very fine-grained as well as systematically collected to be most useful.

Questions About Data Needs

6-1. What is the relative contribution of different sources of error in converting a voter's ballot intention to a final tabulation of votes?

6-2. What data collection must be mandated by states?
6-3. What data are needed to evaluate the performance of electronic voting systems?

PUBLIC CONFIDENCE IN ELECTIONS

Election officials have been very concerned that various election problems in recent election years (most particularly in 2000, and to a lesser extent in 2002 and 2004) have shaken public confidence in elections, with the likely impact of depressing voter turnout in the short term and potentially undermining the legitimacy of government in the longer term.

Questions About Public Confidence in Elections

6-4. What are the factors that influence public confidence in elections?
6-5. How do confidence in and knowledge about elections and voting mechanisms vary across demographic groups?
6-6. What would be the impact on voter confidence of giving independent observers the ability to audit or scrutinize the conduct of an election?

TESTING, CERTIFICATION, AND EVALUATION

The process of testing and certifying electronic voting systems is complex. Yet states and local jurisdictions rely on testing and certification for indicators of whether a system is safe or unsafe to acquire. Today, the process is based on federal qualification and state certification. But the qualification and certification process is cumbersome and slow, and subject to potential conflicts of interest.

Questions About Testing, Certification, and Evaluation

6-7. What are alternatives to the current testing and certification infrastructure?
6-8. Who will conduct testing that is needed beyond what is required by the qualification and certification process?
6-9. What certification requirements, if any, should be imposed on statewide voter registration systems?
6-10. How will election officials respond if, after all is said and done, voters use voting systems that are running uncertified software?

FUNDING AND SUSTAINING IMPROVEMENT

Although the Help America Vote Act of 2002 provided substantial funding for the procurement of new voting systems, it was never intended to assume an ongoing federal role in supporting and operating these systems. Because ongoing operations and maintenance of hardware and software are in general much more expensive than the initial procurement cost, questions arise about long-term sustainability and improvements.

Questions About Funding and Sustaining Improvement

6-11. How will funding be provided for the periodic refreshment of electronic voting systems?
6-12. How will research and development on electronic voting systems be supported and performed?
6-13. What is the impact of evolving standards on deployed electronic voting systems?
6-14. What are the incentives for and barriers to improving electronic voting systems?
6-15. What lessons learned relevant to electronic voting can be found in other regulated industries (e.g., gambling, finance) and government?

ELECTION INSTITUTIONS

Nonelectronic voting systems have had a long history of operation, one measured in decades. But information technologies change much more quickly, and an electronic system used to process the presidential vote in any given year may never be "the same" in any subsequent presidential election.

Questions About Election Institutions

6-16. How can election officials obtain sources of information about electronic voting systems other than the sources provided by vendors?
6-17. How can election officials obtain the knowledge and information needed to respond to and manage change effectively?
6-18. What institutional infrastructure is necessary to support cost-effective use of electronic voting systems over the long term?
6-19. What do the equal protection requirements of voters enunciated in *Bush v. Gore* mean for decisions about voting technologies and their supporting infrastructure?

THE ROLE OF THE PRIVATE SECTOR IN ELECTION ADMINISTRATION

Election administration has never been a function performed entirely by government. Private political associations (interest groups and political parties) have been involved in the administration of elections for a very long time. Private firms have also been increasingly involved in election administration, as in many other governmental functions. For example, private firms have for many years routinely undertaken certain election administration tasks such as the design, layout, and printing of ballots. But local governments are also turning to private firms to provide electronic voting systems, program them appropriately, and repair and maintain them over time. Similar comments at the state level apply to many statewide voter registration databases. For both electronic voting systems and voter registration databases, vendors are often the primary and most important source of expertise.

It is not known whether the involvement of private firms tends to improve election administration in some overall sense. Furthermore, it is not clear whether the role of private firms is increasing across the board. Still, to the extent that private firms are involved in those aspects of election administration that relate to electronic voting systems, a number of important questions do arise, some of which cut across other areas discussed elsewhere in this report.

Questions About the Role of the Private Sector in Election Administration

6-20. What security concerns arise with the intimate involvement of private firms in the operation and maintenance of voting systems?
6-21. What are the roles of vendor certification and a code of ethics for vendors?
6-22. What would be the impact of consolidation among voting systems vendors?
6-23. How will contractual responsibilities be maintained over time (cf. question 5-2)?
6-24. Who owns the data associated with the holding of an election?
6-25. Who bears responsibility for failures or irregularities in the election process?

RESEARCH QUESTIONS

Much of the basic knowledge and information about voting and elections that one might hope had been codified does not exist in a form that is easily accessible or even available.

6-26. What new options (or variants on existing options) do electronic voting systems enable?
6-27. How can electronic voting systems be made more secure?
6-28. What are the operational implications of the voter-verified paper audit trail?
6-29. What special data collection requirements are associated with auditing elections conducted with electronic voting systems?
6-30. What are the costs and benefits of open standards that could facilitate the design of interoperable components for electronic voting systems?
6-31. What are the implications, for security and otherwise, of using multipurpose hardware for voting purposes?
6-32. What would be the desirability and content of a model election code to govern elections undertaken with electronic voting systems?
6-33. How and to what extent have notions of voter privacy and secrecy changed over time and with the introduction of new voting technologies?
6-34. How and to what extent is secure absentee voter registration feasible?

IN CONCLUSION

In developing this report, the committee took note of the significant emotion and passion felt by all participants in the public debate about electronic voting. Although such passion and emotion are often regarded as impediments to a reasoned and thoughtful public debate, the committee believes that these passions reflect—at heart—a very emotional and gut-level commitment to the notion of democracy. One can—and people do—take issue with various arguments about technology or organization, but on balance, the committee believes that the nation is much better served by passionate engagement than by dispassionate apathy, and so the passions expressed by the various participants on all sides of the debate are to be commended rather than disparaged. The committee further hopes that the questions that it has articulated in this report can help the nation overcome political and technological barriers that may impede the improvement of its election systems in the future.

1

The Electoral System

1.1 THE ELECTORAL PROCESS

To set the stage for understanding electronic voting, it is helpful to review the structure of the electoral process itself. Figure 1.1 represents a generic electoral process, and the rest of this section expands on this depiction in words.[1]

The first step in the electoral process for the eligible citizen is **voter registration**. In principle, voter registration establishes a citizen's eligibility to vote. (Voter registration includes everything that is necessary to register eligible voters and to maintain such lists accurately and completely.) States generally require that a voter be a U.S. citizen, at least 18 years of age, and a resident (in some cases, a resident for some minimum period of time, such as 30 days). Most states also limit voter eligibility on the basis of criminal status (e.g., incarcerated felons may not be permitted to vote), and some on the basis of mental competency, although the specifics of these limitations vary.[2] In all states but North Dakota ("states" will be used to denote the 50 states and the District of Columbia, unless

[1]Much of this description is derived from United States Government Accountability Office, *Elections: Perspectives on Activities and Challenges Across the Nation,* GAO-02-3, October 2001. Available at http://www.gao.gov/new.items/d023.pdf.

[2]A description of the legal restrictions on felons and voting rights in a large number of states can be found in American Civil Liberties Union, *Purged! How Flawed and Inconsistent Voting Systems Could Deprive Millions of Americans of the Right to Vote,* October 2004. Available at http://www.aclu.org/Voting Rights/VotingRights.cfm?ID=16845&c=167.

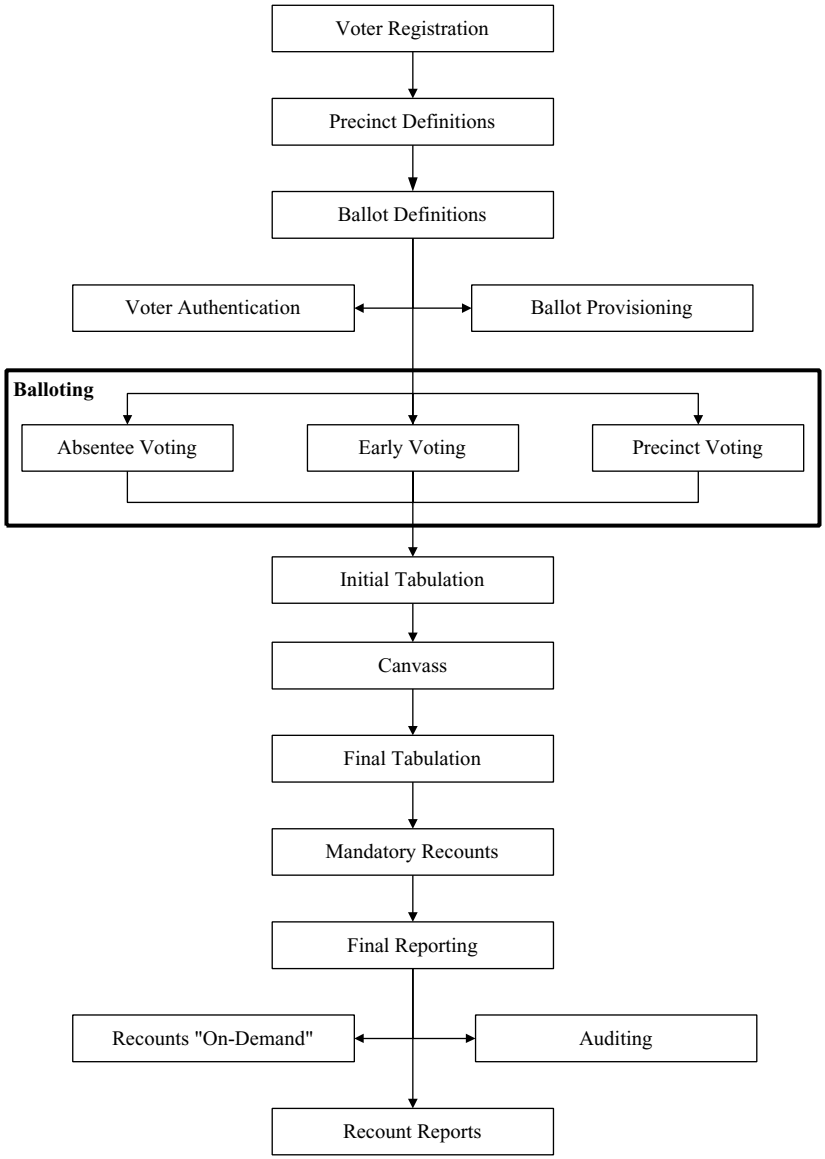

FIGURE 1.1 The electoral process.

otherwise specified), voter registration is only one of several requirements that may be imposed on the right to vote. (North Dakota has no voter registration requirement at all.) Other such requirements include citizenship, age, and residency, though registration itself may be conditional on these factors.

As a general rule, a voter registers to vote in a specific geographic jurisdiction that is determined from the residential address that he or she provides for the purpose of voting. (This address may or may not be the same as his or her domicile, address for tax purposes, or driver's license address.) Citizens can register to vote at election offices. Depending on the state, citizens can also sign up to receive voter registration materials in many places, including motor vehicle authorities and public assistance agencies, or through voter registration drives, or they may download materials from the Internet. These materials arrive, after which the voter fills them out and returns them by mail or in person. The returned materials are accompanied by an original signature that serves as an authentication mechanism when voter registration must be checked in the future. Overseas voters, and members of the U.S. armed forces and their dependents, can sometimes register to vote by fax.

The voting address of record determines the precinct from which the voter casts his or her ballot, whether at the polling place, or by absentee ballot, or by an early vote. A precinct is a subdivision of a local election jurisdiction, and all voters in a given precinct vote at one polling place. (Sometimes, a number of small precincts are consolidated at one polling place, and sometimes election officials can require that all voters from certain precincts vote by mail.) A local election jurisdiction is an administrative entity responsible for the conduct and administration of elections within it, and may be a county or a municipality (a city or town).

Precinct definition is the process by which the boundaries of a precinct are determined by election authorities, based on factors such as the number of voters that a polling place can be expected to serve on Election Day. Precinct boundaries can change from election to election depending on the migration of voters into and out of the precinct and other factors, although they are generally reasonably stable.

Many contests are decided on the basis of the vote in certain geographical regions. Thus, precincts are formed within which all voters vote on the same races and have the same ballots, and so voter registration lists are closely associated with precincts.[3] A voter whose address of record is associated with precinct A, for example, may not be eligible to vote on

[3]Precincts are sometimes associated with more than one ballot, e.g., when citizens must vote in municipal and school races simultaneously.

certain races in precinct B. And, as a general rule, a voter registered in precinct A is not allowed to cast a ballot in precinct B. (Certain exceptions arise in early voting, in which voters from many precincts vote at a central location but receive the ballot appropriate to their precinct of record.)

Ballot definition is the process by which a ballot is created. Ballots indicate the contests (offices and propositions) at stake in an election. In general, these contests are placed on the ballot in an order dictated by state law. Each contest is associated with a specific geographical district; the contests on which a voter is eligible to vote are determined by the collection of districts that contain the voter's address of record. Ballot definition includes incorporation of precinct boundaries that are defined according to state law; a precinct is assigned a union of districts that lie within its boundaries. It is a complex management issue to assure that a jurisdiction is properly divided into precincts and districts in such a way that that the correct contests are associated with the proper street addresses of prospective voters. The result of the ballot definition process is a set of ballot forms for an election, each ballot form differing by at least one contest.

A high priority for election officials is to ensure that a ballot form is clear and usable—voters must be able to navigate the ballot and express their preferences with minimal difficulty or confusion. Accordingly, election officials may print (or display) ballots in many different languages. They concern themselves with displaying or printing the ballot in a way that voters with limited eyesight can read. They put carefully worded instructions on the ballot to guide voters through their choices and try to help them avoid errors. Because voters may be unconsciously biased toward the first or last names on a long list of candidates, some jurisdictions are required to take steps to try to minimize potential biases associated with candidate name placement on the ballot (for example, jurisdictions may randomize the initial ballot position of various candidate names). Another important concern in the ballot definition stage is accuracy—in many elections, the ballot can be long and complicated, and election officials need to make sure that the correct ballot is prepared for each precinct.

Before being entitled to cast a ballot, the voter must "prove" his or her identity to the election official responsible for giving out ballots—this step is known as **voter authentication**. In some locations, voter authentication is as simple as asserting one's name (hence the term "prove" in quotation marks); in other locations, voter authentication involves showing an identification card of some sort.

Then, so that a voter may receive the correct ballot form on which to vote, **ballot provisioning** is necessary. Because the voter is associated with a specific address of record, he or she must receive the ballot corre-

sponding to all races, from local to national, in which he or she is eligible to vote. In addition, the ballot must be appropriately accessible (e.g., presented in an appropriate language or in an alternative form such as audio or Braille).

In casting a ballot, the voter's task is to mark the ballot in accordance with his or her wishes. The marked ballot is the manifestation or expression of the voter's intent for that election. (The expression "marked ballot" originally derives from the idea of marking a paper ballot with a pen. But more generally, the term "marking a ballot" means to record one's voting preferences in some form that can later be tabulated with the ballots of other voters.)

The actual balloting takes place through one of three types of voting. **Precinct voting** refers to voters casting ballots on Election Day in person in the precinct where they are registered to vote. **Absentee voting** refers to voters obtaining absentee ballots before Election Day, filling them out, and returning them to the local jurisdiction (usually by mail) in which they are registered to vote. In some states, absentee voting is allowed only upon presentation of an acceptable reason, such as being absent from the local election jurisdiction on Election Day; being a member of the U.S. armed forces or a dependent; being permanently or totally disabled or ill or temporarily disabled; being over a certain age, such as 65; being an observer of a religious holiday that falls on Election Day; being a student at a school, college, or university; being employed on Election Day in a job whose nature or hours prevent the individual from voting in his or her precinct. In other states, voters can choose absentee voting without presenting any reason at all. In addition, some states allow absentee voters to vote on Election Day as well, on the presumption that the Election Day vote will override the absentee ballot. This approach allows the "last vote cast" to be the one that counts, though it may well entail a greater likelihood of error. **Early voting** refers to voters casting ballots in person before Election Day at some designated location (e.g., the town hall).

Absentee voting in particular is a cumbersome process for election officials because of the requirement that only registered voters should obtain absentee ballots, and it is time-consuming because returned ballots must be authenticated manually. The fact that the mail system is the usual vehicle for transporting ballots and requests for ballots adds another delay to the process. It is sometimes asserted that absentee voting is more subject to fraud and coercion than is precinct voting or early voting. The reason often given is that the in-person nature of voting acts as something of a deterrent, because an absentee voter may improperly vote a second time on Election Day or may have been coerced, or because someone other than the actual registered voter may vote in the stead of the regis-

tered voter, or—much more commonly—because fictitious voters have been invented and registered for the sole purpose of a person intent on committing election fraud obtaining absentee ballots. It is not yet clear whether vote-by-mail or early voting systems in general increase the rate of voter participation (they may simply shift precinct-based voters to absentee voting, for example), but Oregon state officials report that their state's switch to 100 percent absentee voting (that is, the entire election is conducted by mail) did increase voter participation significantly.[4]

Initial tabulation refers to the first round of vote counting. Results from the initial tabulation are the basis for challenges, such as recounts or auditing. The first step in tabulation is sealing the voting machines (or the logical equivalent thereof) to prevent any more votes from being cast after the polls close. Then, totals for the polling location are ascertained and produced for the individual precincts if the polling location supports more than one precinct. The process used varies from jurisdiction to jurisdiction and depends on the particulars of the voting technologies involved. The votes from each precinct may be counted at the precinct or in a central location. Most states require a polling place total to be generated and in some states, the totals are required to be posted. For both central count and precinct count systems, the polling location information is transferred to a central location for tabulation or aggregation of the precinct subtotals. Also, votes cast through absentee or early voting must be counted as well, and these are mostly typically counted at the central location.

Final tabulation (also known as the canvass) usually takes place some days after Election Day and refers to vote totals that have been obtained from a careful canvass of all votes by precinct, resolving problem votes, and counting all valid votes (votes cast through absentee and other pre-Election Day processes, votes cast on the regular Election Day, and valid votes cast provisionally during Election Day). In practice, unless the election outcome is contested, the canvass also includes a reconciliation of the poll books (noting who showed up to vote) against the total number of ballots counted. In addition, some states require a certain percentage of paper ballots be hand counted to validate the tabulation program for paper systems as part of the canvass. The results of the manual hand count are compared with the tabulated results for a precinct and must agree with those tabulated results within a specific margin of error. In other instances, a recount is mandatory under state law if the margins are sufficiently low.

[4]See, for example, Priscilla Southwell, "Five Years Later: A Re-assessment of Oregon's Vote by Mail Electoral Process," *Political Science and Politics* 98(1): 89-93, 2004.

A **contested election** occurs when the outcome of an election is challenged and someone alleges fraud or misconduct on the part of a candidate, voters, or election officials or systems/process failures. The basis for the challenge is analyzed and the responsible election or judicial official must determine what actions are required to resolve the allegations. A contested election usually includes a more complete **audit**, which seeks to validate and verify as many aspects of the election cycle as possible without violating state privacy laws, and in particular an audit cannot use data that might associate a specific voter with a specific ballot. The most well-known action to result from a contested election is a **recount** of the votes, but this is only one of the actions that an audit may entail.

Procedures for determining whether a recount is necessary vary by state. In some instances, losing candidates in an election generally have some opportunity to contest an election and demand a recount if the margin of loss is less than a certain percentage of the vote. Recounts can involve machine retabulation of the ballots for one race, or all races, verifying the totals for each candidate or choice and/or hand counts of additional individual precinct totals in sufficient number so as to narrow the statistical margins of error. Note also that recounts (i.e., retabulations) per se do not usually change the outcome of elections—when outcomes change, it is usually for other reasons (e.g., in the 2000 presidential election in Florida, the count changed because of the way voter intent was interpreted on cards, not because of a difference in the machine count).

The primary challenges for election officials in audits arise when vote tabulation systems or human vote counters are unable to infer voter intent from the marks that are recorded on ballots, resulting in uncertain counts. For example, a voter may circle a candidate's name on an optical scan ballot rather than filling in the box beside the candidate's name. From the voter's perspective, this may be a perfectly reasonable way to indicate a preference, but most optical scanning devices are not able to record the circling of a candidate's name as a vote cast for that candidate. In some states, elections officials are required by law to resolve ballots according to a determination of the voter's intent in casting a ballot. In other states, voter intent is irrelevant, and an ambiguous ballot is resolved (or discarded) on the basis of the marks that actually appear on the ballot.

In addition to the above (recounting ballots, determining voter intent on ambiguous ballots), an election audit may also include challenging voter registration rolls, which includes the number of voters disqualified at the polls, those disqualified during registration, and those denied absentee ballot requests; reviewing the disposition of provisional ballots; and determining whether voters received the correct ballots. Note also that the specifics of what is actually involved in dealing with a contested election depend on the allegations made in contesting it.

In many states, voters are not by themselves effectively able to request recounts. In addition, there are significant hurdles and barriers in many states for candidates to request recounts, such as raising sufficient funds to cover the high costs that may be required by a recount.

Certification refers to the process through which a designated official certifies the final vote totals for each candidate and each issue on the ballot, within a specific time frame.

Upon completion of final tabulation and certification, the process of election administration returns to voter registration. Based on activity in the just-completed election, voter history files are updated, and voter registration lists may themselves be updated based on voter inactivity or on other information about changes in voter status learned in the previous election. Election administration is thus a dynamic process, with the updated voter registration database constituting the foundation on which the next and future elections will be based.

1.2 SCALE OF THE ELECTORAL SYSTEM

In the United States, there were 206 million Americans of voting age in 2002,[5] of which 156 million were registered to vote. In the 2002 election, 80 million cast ballots, in approximately 9,500 voting jurisdictions. These 9,500 voting jurisdictions were divided into approximately 185,000 precincts; a total of about 800,000 voting machines were deployed in these precincts.[6]

To assist these voters, about 1.4 million poll workers provided Election Day assistance and supervision of the polls. Collectively, the election enterprise costs the states an estimated $1 billion per year.

The federal legal context for elections has three components. The first component is the basic framework for elections contained in the Constitution of the United States, which gives responsibility for elections primarily to the states. The second component is the result of three pieces of legislation—the Voting Rights Act of 1965, the Uniformed and Overseas Citizen Absentee Voting Act of 1986 (UOCAVA), and the National Voter Registration Act of 1994 (NVRA)—which collectively set additional parameters on the federal oversight of election administration.

The third component is the Help America Vote Act of 2002 (HAVA). Although the implications and mandates of HAVA are still evolving, HAVA in some ways marks a new federal role, empowers the states to

[5]This figure includes many who are of voting age but ineligible to vote for a variety of reasons, including felony convictions, noncitizenship, and mental incapacity.

[6]Statistics regarding voter turnout and related information are taken from the Election Assistance Commission Web site, http://www.eac.gov/election_resources/02to.htm.

take a stronger role vis-à-vis local election officials, and also updates or changes some aspects of the UOCAVA and NVRA legislation. The philosophy underlying HAVA, though not HAVA's detailed requirements, was inspired by issues that came to light in the Florida recount in 2000 and the decision, which effectively decided the 2000 presidential election. *Bush v. Gore* held that equal protection requirements under the 14th Amendment meant that voters in one local election jurisdiction of a state could not be treated differently than voters in another jurisdiction of that state, and, in particular, that similar methods of counting votes had to be used for all local election jurisdictions across the entire state, thereby minimizing the discretion that could be exercised by individual jurisdictions. Together, HAVA and the *Bush v. Gore* decision suggest that a greater degree of uniformity within individual states may be forthcoming in the future.

These four pieces of federal legislation are described in Box 1.1.

1.3 OBSERVATIONS

Conny McCormack, the chief election official in Los Angeles County (which is the nation's largest and most complex election jurisdiction) often compares conducting an election in her jurisdiction to a major military mobilization.

> Akin to a major military deployment, the logistics of administering a statewide election in Los Angeles County is without equal. We have secured more than 3,000 polling locations, recruited and trained 23,000 poll workers, registered and updated records for many thousands of voters who are eager to participate in the General Election, and mailed sample ballot booklets to 3.7 million registered voters. On election night we will count 2+ million ballots.[7]

This commentary provides a quick introduction to the logistical challenges associated with running a modern election in a large, urban election jurisdiction. But there is little general realization that modern elections are difficult to administer effectively, regardless of the specific problems in any particular election jurisdiction. The administrative difficulties are rooted in a number of dilemmas that election officials face; four of the most important are time, resources, complexity, and the law.

Time pressures are acute in the business of election administration. Unlike many areas of governmental activities, there are many time-sensi-

[7]Conny McCormack, *Elections: FYI 2004, Presidential General Election, November 2, 2004, An Informational Manual to the 2004 Presidential General Election for Media, Community Organizations and Interested Citizens,* Office of the Los Angeles Register-Recorder/County Clerk.

Box 1.1
Federal Legislation Relevant to Elections

• *The Voting Rights Act of 1965* prohibits voting practices and procedures, including redistricting plans and at-large election systems, poll worker hiring, and voter registration procedures, that discriminate on the basis of race, color, or membership in a language minority group or that have a racially discriminatory impact. In addition, it enables the federal courts and the attorney general to assign federal examiners and federal observers to voting jurisdictions alleged to engage in discriminatory practices, and allows the provision of voting assistance to voters who are blind or illiterate or who have disabilities.

• *The Uniformed and Overseas Citizen Absentee Voting Act of 1986* (UOCAVA) requires that the states and territories allow certain groups of citizens to register and vote absentee in elections for federal offices. In addition, most states and territories have their own laws allowing citizens covered by UOCAVA to register and vote absentee in state and local elections as well.

• *The National Voter Registration Act of 1994 (NVRA—the so-called Motor Voter Act)* requires states to provide individuals with the opportunity to register to vote at the same time that they apply for a driver's license or seek to renew a driver's license, at all offices that provide public assistance or services to persons with disabilities, and by mail using mail-in forms developed by each state and the Election Assistance Commission. The NVRA also creates requirements for how states maintain voter registration lists for federal elections. States must notify voter registration applicants of whether their applications were accepted or rejected, keep voter registration lists accurate and current, and apply specific safeguards intended to keep voters from being improperly purged from voter registration lists (e.g., a voter should be purged only upon conviction for a disqualifying crime or being adjudged mentally incapacitated and only when state law provides for such removals).

• *The Help America Vote Act of 2002* authorizes funds to be appropriated to states to replace old voting systems and to purchase additional voting systems for persons with disabilities. It establishes the Election Assistance Commission, mechanisms to define voluntary standards for voting systems, and mechanisms to certify voting systems that conform to these standards; directs the states to establish statewide voter registration databases; and imposes specific requirements on the purging of these databases.

SOURCE: These thumbnail descriptions are derived from the Web sites of the Department of Justice (http://www.usdoj.gov/crt/voting/) and the Election Assistance Commission (http://www.eac.gov).

tive activities that election officials must engage in that make for administrative headaches. Elections are held on certain mandated dates, and election officials are strongly pressured to produce preliminary tabulations of vote totals quickly after polls close and final tabulations within just a few weeks of holding a major election. An example of such time pressures was recently seen in the City of Los Angeles, when the final returns for a mayoral primary election were held up until the early morning hours owing to logistical difficulties in getting ballots to the central tabulation location. The candidates competing in this election and the media covering the race all complained loudly about the delayed vote count (which was nearly complete by 4:00 a.m., hardly a long wait!).

But there are also significant time constraints before the election is held. There are filing deadlines for candidates who want their names on the ballot, and once the basic parameters of the content of the ballot are clear (in some cases just weeks before the election is held), ballots must be defined (that is, laid out), tested, and prepared for the election. Absentee ballot applications must be received, requests processed, and ballots sent to qualified voters so they have time to vote and return their ballots. Final lists of registered and eligible voters must be prepared, a difficult task in many places with the close of registration now only a few weeks before the election. And in-person early voting must be conducted before the election. Obviously, all of these tasks occur under significant time pressure.

Resources are a major source of election complications. Many of the tasks associated with election administration are undertaken by entities over which the election official has little control. For example, much of the task of registering voters and providing absentee ballot applications is done by political parties or organized interest groups. Also, election officials must rely upon scores of volunteers or nominally paid workers on Election Day, for tasks from facilitating precinct voting to assisting with tabulation activities once the polls close. Thus, election officials need to be concerned about having enough people to staff poll sites, and they also have to be very concerned about the quality of the work that that these volunteers or poorly paid employees conduct. Because election officials are forced to rely upon the work of individuals or entities over which they have no or only loose control, the task of election administration is greatly complicated.

Election administration is also quite complex. The complexity of the election process is largely invisible to most of the public; tasks that on the surface would seem to be simple to undertake, like checking the validity of a voter registration request, can become quite complicated, and can result in legal challenges and court proceedings. Election officials must maintain an accurate voter registration list, a list that needs frequent updating and revision. Addresses must be standardized throughout the

state, and responsibility for making updates must be assigned and carried out. They must use this registration list to determine voting precincts and to ensure that the ballots used in each precinct include only the races that those voters are eligible to vote in. They must allow for early and/or absentee voting before Election Day, and ensure that no eligible voters are allowed to cast more than one ballot. They must have mechanisms to allow voters to cast provisional ballots, and to have these ballots authenticated before they are tabulated. And this basic task is in many places repeated two or three times a year (sometimes even more frequently).

The last layer of difficulties facing election administrators comes from the vast and growing body of election law. Election officials need to comply with a web of federal, state, and local laws and regulations. They must ensure that basic federal laws, such as the Voting Rights Act of 1965, are followed. They need to follow state law, regulations, court rulings, and state and federal administrative actions, and they must ensure that local rules are obeyed. And they need to stay abreast of new legal and regulatory developments, such as the passage of new federal and state rules to accommodate new voting systems.

2

Public Confidence in Elections

2.1 THE RELATIONSHIP BETWEEN DEMOCRACY AND ELECTIONS

A fundamental characteristic of democracy—perhaps its defining characteristic—is that government derives its legitimacy from elections. For example, the *American Heritage Dictionary of the English Language* (fourth edition) defines democracy as "government by the people, exercised either directly or through elected representatives."[1]

Given the central importance of elections to democracy, it is axiomatic that elections are high-stakes affairs. The stakes are further increased by the majority-rule nature of most elections in the United States—in principle, even one vote out of tens of millions cast can determine the outcome of an election, because victory depends only on a candidate winning a majority (or a plurality) of the votes cast.

2.2 LEGITIMACY IN A DEMOCRACY

Democracies derive their legitimacy from elections that the people collectively can trust. In turn, legitimacy is important for the long-term functioning of a democratic society, because it is what underpins the willingness of the losers in an election to abide by policies set by the winners (with whom the election losers are likely to disagree). In other

[1]See http://www.bartleby.com/61/34/D0123400.html.

words, although elections do determine in the short run who will be the next political leaders of a nation (or state or county or city), they play an even greater role in the long run in establishing the foundation for the long-term governance of a society. Absent legitimacy, democratic government, which is derived from the will of the people, has no mandate to govern.

While many factors contribute to the legitimacy of a government,[2] one sine qua non is undoubtedly that elections are perceived by both winners and losers as free and fair. Indeed, it is often said that the main purpose of election fairness is to convince the loser that he or she lost the election fair and square—winners rarely complain about the fairness of an election. Perhaps more important, these comments apply even more strongly to the electorate supporting the losing candidate.

Of course, the process is greatly complicated by the fact that the electoral process will undoubtedly yield some sore losers—individuals who disguise their unhappiness over the outcome of an election with complaints about unfair process, even if the election was conducted under the fairest of circumstances and rules and procedures. Similarly, winners and especially their supporters are likely to invoke the spectre of sore losers, even if complaints about election fairness have some reasonable factual basis. Finally, an important psychological issue is that as a general rule, individuals—that is, voters—tend to associate with like-minded individuals and to read newspapers and other information sources that reinforce their own predispositions. This tendency reinforces their perceptions of being in the majority. Thus, they are likely to see an election loss more as the result of election chicanery than as a fair loss.

The political environment of today compounds the issues described above. Perhaps most significantly, political campaigns and debates today are rancorous and bitter, a throwback to the political climate that existed in the United States over 100 years ago.

This rancor sets the tone for much of the following:

- Most governors and state officials are elected from the ranks of one party or another. They are thus partisan officials by definition, and these officials are ultimately responsible for state operations, including the conduct of elections. When such officials make decisions that benefit—or can be seen to benefit—candidates from their party, suspicion on the part of

[2]For example, legitimacy may be undermined by gerrymandering in congressional districts and by partisan election officials who certify an election in favor of their own party amidst doubt about fairness of the election.

the opposition is natural. In today's highly charged political environment, these tendencies are sometimes accentuated, and there is often little shared trust that partisan officials can make nonpartisan decisions.

- Close elections—much more likely when the electorate is about evenly divided—are breeding grounds for postelection suspicion, on the theory that even a small amount of deliberate fraud or accident or mishap or improperly followed procedure might have tipped the election the other way. While the presidential election of 2000 is perhaps the most salient example, outcomes in other close races have been very closely scrutinized by supporters of the losing side for irregularities.[3]
- The cost of political campaigns has risen. In the primary elections of some jurisdictions, it exceeds $100 per vote received and has led some analysts to wonder if it raises the incentive to cheat.
- Vendors of electronic voting systems have not always been seen as politically neutral. In an environment in which questions are raised about whether such systems are actually trustworthy, partisanship manifested in the vendors of these systems is likely to raise suspicion.

In such an environment, where the perceptions of fairness can depend on whether your side won or lost, a more reasonable objective is the notion of a "trusted" election, where "trust" entails a factual basis for that trust. That is, a trusted election process is one that works, can be shown to have worked after the election has been held, can be shown to have not been manipulated and to have not led to a large number of mistaken or lost votes, and can be shown to reflect the intent of the voters. To the extent that there is a provable and factual basis for calling an election trusted, there is at least a chance that more people will consider the election fair, even if their side lost.

Put differently, the fact that in the U.S. system of government, partisan office-holders are ultimately responsible for the conduct of elections (or can exert strong influence over elections) makes very important indeed the existence of procedures and practices that demonstrably minimize the possibility that these officials will be able to improperly affect election outcomes. To the extent that public trust in the integrity of elections is diminishing, the importance of such procedures is magnified.

[3]Stories from 2004 along these lines include the gubernatorial race in Washington state (in which the governor's race saw a margin of a few hundred votes in both directions before the winner was finally determined in court and the loser chose not to further contest that court decision), and the presidential race in Ohio.

2.3 DESIDERATA FOR ELECTIONS

With the foregoing in mind, consider the goals that elections must serve. The committee believes that there would be little disagreement about the following as election principles or goals:

- Voters are entitled to secrecy in the ballots they cast, both as they cast them and in any subsequent counting of votes.[4] (With voting secrecy, voter coercion becomes effectively impossible.)
- A voter may cast only the number of votes in any given race for any given office or any given ballot proposition to which he or she is legally entitled. In general, this is one vote per race, although there are exceptions to this rule—for example, where voters can cast more than one vote for more than one candidate on a list of more than two or in instant runoff elections.
- A voter may cast a vote only for offices or propositions for which he or she is legally entitled to vote.
- A voter may not sell or trade his or her vote.
- All voters legally entitled to vote, but only those voters and no one else, should be allowed to vote.
- All cast ballots should be counted accurately.
- An eligible voter will not face undue obstacles in casting his or her ballot, regardless of her or her personal circumstances (e.g., level of literacy, physical or cognitive disabilities, education, place of residence).
- The system on which voters cast ballots will be operable for the entire time that the polling place is open.
- Audit trails and other records will be kept to monitor the extent to which these principles are honored (but not at the cost of violating voter secrecy).
- The election system will produce an unambiguous and definite winner even in close races (Box 2.1).

Though these desiderata are widely accepted, they are not, in practice, of equal importance. While very few election officials and administrators would admit to breaches of voter secrecy on even a small scale, most would acknowledge that proper procedures may not have been

[4]Note that secrecy in this context is not necessarily a binary concept. One operational definition for the secrecy of a given ballot is the number of other ballots that are irreversibly mixed with that ballot. In an election with one vote cast, no degree of secrecy is possible. In an election with three votes cast and a 2 to 1 winning margin, the single person casting the minority vote has less privacy than a voter casting a vote for the minority side in an election in which 300 votes are cast and the winning margin is 200 to 100.

Box 2.1
Close Elections and Irreducible Errors

The requirement that election systems produce a definite winner has historic roots. Elections determined by simple majorities (or pluralities) made sense when the number of voters participating in elections was small—with small elections, errors could be minimized enough that recounts could be expected to result in more accurate vote counts even in very close elections. But as the number of voters in an election increases, it is inevitable that the potential for miscounts of some sort will also grow. Good election technologies and procedures can reduce the magnitude of the likely error in the vote count, but it is virtually impossible to believe that the error can be reduced to zero consistently in all elections.

Today, some states mandate that margins of less than a certain percentage (e.g., 1 percent) trigger an automatic recount. Recounts triggered under such conditions recognize that margins of victory under a certain percentage are inherently clouded, and that measures need to be taken under such circumstances to validate the legitimacy of the election.

If one denotes the magnitude of the irreducible error as *x* percent of the total vote, an election that produces vote totals that are within *x* percent of each other is for all practical purposes a tie, and no amount of recounting or auditing will discern the intent of the voters more accurately. Thus, although a mandate to decide such elections by lottery or tossing a coin would be highly controversial (and the committee is silent on the ultimate overall desirability of such a mandate), it would be more faithful to the underlying reality that some degree of irreducible error inevitably exists.

How should an appropriate value for *x* be determined? To be sure, statistical analysis plays an important role here, as does historical and operational experience. But ultimately policy makers will have to determine the appropriate value. Perhaps of more importance would be an agreement by all candidates—in advance of the election and as a condition for being allowed to run in the election—to abide by a requirement to settle the election by lottery should this "statistical" tie occur.

followed to the letter on a given Election Day, that some properly registered individuals may have been turned away at the polls, that some votes cast may not have been recorded, that ballots cast do not reconcile with votes tallied, and so on. They would further argue that with limited resources, they do the best they can—and that with more generous resource allocations they would be able to do better.

The desiderata described above provide a framework for understanding electronic voting systems and how they fit into the larger societal, organizational, and institutional context of election administration. For example, they drive many of the technical requirements for electronic voting systems, as well as the opposition to electronic voting systems from many quarters.

3

Voting Technologies

3.1 INTRODUCTION

Mechanical devices started to replace hand-marked paper ballots in the late 1800s, and the use of the pointer/punch card system to record votes dates to 1892. Some form of this method remains in use throughout most of the nation today, with as much as a third of the population still voting with punch card systems. By automating vote counting, punch card systems greatly speeded vote tabulation/counting and somewhat reduced the potential for error and fraud as compared to hand-counted paper ballots, but systematic machine error and intentional damage to or tampering with voting or tabulating equipment remained possibilities. (In addition, certain punch card systems may have increased the number of failures to record voters' intentions because of the poor feedback available on these systems.)

A variety of electronic voting systems have been proposed to further increase the efficiency of election administration and reduce the problems and errors associated with nonelectronic systems. In the public debate, the term "electronic voting system" has been used to refer to a computer-based voting station located in the polling place with which citizens interact directly to cast their ballots—that is, in common parlance, an electronic voting system is an electronic ballot marking system. This report is mostly about electronic ballot marking systems, but will generally use the term electronic voting system in deference to common usage except when the ballot marking function needs to be emphasized. Nevertheless, it is

important to note that computer-based systems can and do support the electoral process in at least three other important ways:

- *Computer-based voter registration databases*. Today, almost all registration is done with such systems; nonelectronic systems are now the exception and they will be essentially nonexistent as of January 1, 2006, if the Help America Vote Act of 2002 mandates for voter registration databases are met.
- *Electronic vote tabulation systems*. These administrative systems tabulate the individual ballots cast by voters, regardless of how those votes were recorded or indicated. With some types of ballot, these tabulation systems are responsible for determining how the marks on the ballot should be interpreted. Voters do generally not interact directly with tabulation systems.[1]
- *Ballot definition systems that determine all of the contests that are relevant to specific precincts*. As noted in Section 1.1, ballot definition is often a complex process because the geographical districts associated with specific electoral contests are not identical to precincts, and any precinct may contain several districts. Computer-based systems greatly simplify the administrative task of ballot definition.

Even from the brief description above, it should be apparent that computer technology and voting and elections intersected long before the public debate about electronic voting systems came to the fore. But as often happens, the importance and greater visibility of the electronic ballot marking systems that voters use directly have highlighted both the potential problems and the new opportunities—and both problems and opportunities are now at the center of the public debate.

All ballot marking systems are expected to meet a number of different goals. They should be low in cost to purchase, operate, and maintain over their entire life cycle. They should be efficient and secure in their operations to provide accurate counting and produce the fast results required by the press, contestants, and voters. Ballot marking systems should minimize voter errors including overvoting, undervoting, and unintended voting. (In overvoting, the voter indicates more than one choice for a single-choice contest, thus invalidating his or her vote. In undervoting, the voter indicates no choice for a given contest. Undervotes are entirely legal, and there is no way of distinguishing between a voter's choice to

[1]In some cases (in particular, with direct recording electronic systems), the ballot marking system incorporates a local tallying function that totals the votes cast on individual stations. The central tabulation facility thus tallies results from individual voting stations.

refrain from voting in a particular contest, an error of omission on the voter's part, or a vote that a system fails to capture somewhere.) Ballot marking systems should safeguard the secrecy of a voter's ballot. They also should be easy to use and accessible to all voters regardless of age, language capabilities, physical abilities, or level of experience. Note also that some of these goals may be inconsistent or at least in tension with each other.

When the ballot marking systems in question are electronic, other goals may be added. For example, one might argue that they should be as transparent as possible in their operation, or that they should be resistant to disruptions in service caused by externalities such as power failures, or that they should actively guide voters through the ballot, or that they should intervene to recognize, block, and help users recover from errors. Because experience with electronic voting systems is much more limited than experience with nonelectronic systems, there is less consensus on the relative desirability or importance of any of these goals compared to other goals.

It is easy to see why electronic voting is appealing to election officials. For many jurisdictions, electronic voting promises significant reductions in the logistical burdens of election administration by reducing the volume of paper that must be managed. Electronic transmission of results from the local precinct to the central tabulation authority offers the possibility that election results can be known much more rapidly. Certain possibilities for fraud—in particular, those that were most common in the past with hand-counted paper ballots or mechanical voting devices—are greatly reduced, because the expertise needed for committing such fraud is greater and the media involved are different. Where the voter is using an electronic ballot marking system, the possibilities of voter error may be reduced, as electronic voting machines can be programmed to check for common voter mistakes such as overvoting and because these voting systems can reduce the need for subjective assessments of potential voter intention. For such reasons, election officials are favorably predisposed toward electronic voting, making it likely that over the long run, electronic voting systems will supplant nonelectronic voting systems. But acknowledging this trend over the long run does not mean that acquisition of such systems should happen before important questions about these systems are resolved. It is in this spirit that the questions of the report are offered.

Electronic voting systems also have unique characteristics from security and usability perspectives. From a security perspective, the complexity of the technology involved means that the expertise required to commit election fraud is greater, as compared with nonelectronic systems. With greater expertise required, fewer people are thus capable of perpe-

trating election fraud. Moreover, because voting systems are deployed to the field essentially as sealed boxes, possibilities for committing fraud in electronic systems are limited to points of high leverage, such as central storage depots, a vendor's distribution facility, or the vendor's software development shop. On the other hand, the magnitude of the fraud possible becomes large under these circumstances—and because electronic voting systems operate on electronic signals rather than with physical documents, the detection of fraud is potentially more problematic.

From a usability perspective, electronic voting systems offer programmable user interfaces. Programmability means that there are many more options for presenting ballots to voters. With many more presentation options, a much higher degree of customization to voter needs or preferences is possible. Programmability also enables more rapid prototyping and testing and easier modification of ballot interfaces. And, appropriately programmed electronic voting systems are also capable of monitoring user behavior and can thus intervene to block certain kinds of errors or to actively help users with interface problems. On the other hand, a large number of options for presenting a ballot means that there are many more possibilities for getting some aspect of the interface wrong, and thus many more opportunities for potential confusion or outright mistakes. In addition, some voters perceive the "disconnect" of the interface from the tabulation mechanism as a potential source of fraud, and so programmable interfaces may contribute to lessened confidence in the voting system.

3.2 ELECTRONIC VOTING SYSTEMS IN USE TODAY

As a baseline for understanding the characteristics of electronic voting systems, consider the traditional paper-based voting system. In this traditional system, voters cast their ballots by marking forms that have the names of candidates printed on them. These forms are tabulated manually and have no computer-assisted error checking. Unlike other types of voting systems, paper ballots can accept different marks on them and still be comprehensible to the human being who reads them. On the other hand, the fact that a human being is involved in tabulation means that tabulation is slow when many ballots must be counted, and also that subjective human judgment is involved in interpreting ambiguous marks on the ballot. When large numbers of voters, multiple languages, and complex ballots are involved, hand-counted paper ballots are especially inefficient.

A second kind of traditional voting system is the lever machine. Such machines are based on the use of a ballot that is posted in the voting booth to indicate the correspondence between lever and candidate or proposition. The vote tabulation in the precinct is mechanical, not computer-

assisted, and central counting is not possible. Lever machines prevent one type of voter error—overvotes. Obviously, they cannot be used for absentee ballots. Furthermore, lever machines are no longer manufactured, which contributes to their high overall costs.

These two voting systems—hand-counted paper ballots and lever machines—do not use computers in any stage of the process, although even with these systems, computers—or at least calculators—must be used to tally long lists of numbers. Of course, the introduction of electronics and computer technology expands enormously the options for the design of voting systems.

In the United States, there is a wide diversity of electronic voting systems currently in use. All of these systems use computers to tabulate votes, including systems that are entirely manual from the standpoint of accepting user input.[2] Some systems also use computers as the input device used by the voter for casting a ballot.

An important distinction in these systems is how the system enables the voter to verify that his or her vote is indeed captured as intended. The revised Federal Voting System Standards distinguish between direct and indirect verification of a vote.

Direct verification is voter verification that is mediated through a human sense, such as vision. That is, the voter's actual ballot—with votes recorded on it—can be directly viewed by the voter, and his or her votes as recorded can be checked by the voter to see that they are correct without the mediation of any other device. Direct verification thus provides substantial (and tangible) evidence for the voter that his or her vote has indeed been captured by the marked ballot as intended. Today, direct verification systems are based on punch cards and optical scanning.

- *Punch card systems* are based on a physical document ballot and computerized vote tabulation. In one system, the voter uses a stylus to punch holes in the card at the appropriate positions to indicate his or her vote; this system can be used for absentee voting as well. In addition, the most commonly used form of punch card itself does not have names printed on it, and so the correspondence between a given hole and the appropriate candidate must be assured by the proper physical alignment of the card in a holder or bracket. Furthermore, it is virtually impossible for a voter to verify that his marks on this type of punch card correspond to his actual choices without going to a great deal of extra effort to match

[2]Approximately 86 percent of all votes in the 2004 election were counted by computer (all votes except those cast by paper or lever). By contrast, about 29 percent of votes were cast electronically. See Election Data Services, *Voting Equipment Summary by Type as of 11/02/2004*. Available at http://www.electiondataservices.com/VotingSummary2004_20040805.pdf.

the numbers on the punch card with the numbers in the informational booklet for voters. In another, less widely used punch card system, a special device is used to punch holes in a ballot card with the names printed directly on the card. For both systems, multiple punch cards must be used for long ballots.

- *Optical scan systems* (sometimes called Marksense systems) are based on a physical paper ballot on which votes are indicated by the appropriate marks. An optical scanner then reads these marks when the ballot is fed into it, and votes are tabulated electronically. In the most common instances, these marks are made by the voter's hand (e.g., by using a pencil to fill in an oval or to draw a connecting arrow for each contest). Because marks are made by hand, optical scan systems can be used for absentee ballots. Only a narrow range of ballot marks can be read by the optical scanner, and so a voter may be in the difficult position of not knowing exactly what marks will be read properly by the machine.

For both punch card and optical scan systems, it is possible for voters to cast invalid ballots (e.g., if more than one candidate is chosen for a one-person race), though in-precinct counting at the point of voting can warn the voter that an invalid ballot has been cast (so that he or she may try again). Warnings of undervotes can also be provided.[3] When centralized counting (at the central tabulation facility) is used, opportunities for real-time error correction are lost, although in the case of optically scanned ballots, the jurisdiction can organize a committee to infer voter intent on improperly marked ballots (if permitted by state law).

A further subtlety is that a voter may have directly verified that he or she has marked the ballot as intended, but such a mark may not correspond to a vote that is machine-readable. For example, a voter who circles names on an optical scan ballot when a valid vote is indicated by a filled-in bubble can verify that the correct names are circled, but the votes on the ballot will not be recorded by the scanner.

Indirect verification refers to voter verification that is mediated electronically. That is, the voter's ballot is recorded on some computer-readable medium and electronically displayed back to the voter for verification. In this instance, the voter must trust that what is displayed for verification is indeed what the system has captured.

The canonical indirect verification system is the direct recording electronic (DRE) system. A DRE system allows the voter to make his or her

[3]In practice, warnings of undervotes are often not provided, for two reasons. First, voters have a right to undervote, and so a public indication of an undervote might be regarded as an invasion of a voter's privacy. In addition, the check for an undervote often slows down the voting process significantly, so election officials often do not activate such a feature.

choices and, when the voter is finished voting, provides the voter with the chance to verify all the votes cast and then records the votes when the voter takes some affirmative action to finalize the ballot. Indeed, the earliest DRE system could be described as an electronic version of the lever machine: the entire ballot appeared on a single sheet, microswitches lit up when pressed, and voters were required to cast the ballot at the end. In general, modern DRE systems rely on a display screen to present the ballot to voters. For accepting input, some use touch screens, while others use mechanical selection devices. DRE systems enforce ballot logic in real time at the point of voting, can perform error checking to inform the voter of overvotes and undervotes, and can prevent the voter from improperly marking his or her ballot. Because they are programmable devices, displays and other user interfaces can accommodate a variety of user needs, and DRE systems are thus potentially the systems that are the most usable by people with various disabilities. Unless they are specifically designed to do so, DRE systems cannot be used for absentee voting (but see Box 3.1). If only initial purchase costs are taken into account, DRE systems are among the most expensive of all voting systems on the market, although no one knows what the total unsubsidized cost of ownership and operation of such systems is over their lifetime.

Finally, a number of other electronic voting systems attempt to merge the strengths of both direct and indirect verification. Direct verification has the advantage of being an unmediated interaction between voter and ballot. Because the voter-ballot interaction in indirect verification systems is mediated electronically, such systems can also count ballot results electronically, without the need for human intervention. These combination systems also create the physical record contemporaneously with the casting of the (electronic) ballot rather than creating the records after the polls close from the electronic records stored on the voting device, and many electronic voting skeptics believe that contemporaneous creation provides a high degree of traceability from the voter's intent to ballots that can be physically counted.

With a physical record in hand, vote tabulations can be undertaken in principle repeatedly should they become necessary (e.g., if a recount is necessary). At the same time, it must be recognized that the mere existence of a physical record of a vote does not guarantee that it can be read unambiguously. Indeed, recall that the dimpled and hanging chads of the 2000 election were associated with a system based on physical records—the punch card. A laser printer that prints documents will eventually run out of toner, and the documents printed near the end of the print run may be faded and unreadable. A thermal fax printer might print a record that fades over time with exposure to light. Such problems can be ameliorated at sufficient expense, but it is unrealistic to assume that they can be eliminated.

Box 3.1
The Secure Electronic Registration and Voting Experiment (SERVE)

In 2004, the Department of Defense (DOD) initiated planning for conducting a prototype-based experiment, the Secure Electronic Registration and Voting Experiment (SERVE), which would have enabled certain American citizens living outside the United States and military personnel and their dependents wherever they were living to register to vote in their local communities (in the United States) and to vote in the elections for those communities.

The system developed for SERVE would have enabled a voter with proper authentication credentials to register to vote, and then to vote, from any modern Internet-connected, Web-enabled Windows-based personal computer. The local SERVE application (downloaded from a secure central server) would have interacted with that central server. The central server would have been responsible for authenticating the voter's credentials, presenting the correct ballot through the Web browser from the appropriate community, receiving user input representing his or her votes, and transmitting the records of every individual vote cast to local election authorities in the appropriate community. An application running in those communities would then integrate the cast vote records received with votes cast in polling places and by mail.

In its initial form, SERVE was intended to provide electronic registration and absentee voting services for voters in 51 jurisdictions in seven states that had agreed to participate. DOD had expected to serve about 100,000 votes over the course of a 1-year experiment, including both the primaries and the general election. Information obtained from this experiment was to have been used to provide these services in the future to all overseas and military voters and their dependents.

In early 2004, the DOD canceled the SERVE experiment, citing security reasons for its termination.[1] However, in the FY 2005 Defense Authorization Bill and taking note of security issues, Congress directed the DOD to try again, after the Election Assistance Commission promulgates guidelines for electronic absentee voting and voter registration.

[1]An analysis of the security of SERVE can be found in David Jefferson et al., *Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*, January 20, 2004, available at http://www.servesecurityreport.org/.

An example of a combination system might be an electronic voting system that prints a properly marked optical-scan paper ballot. The electronic part of the system would be indirectly verified (and processed entirely electronically), while the printed optical-scan ballot can be counted using the techniques used for all optical-scan voting systems. Box 3.2 describes another example that is more commonly discussed—the voter-verified paper trail.

Box 3.2
On the Voter-Verified Paper Audit Trail

In 2004, the notion of the voter-verified paper audit trail (VVPAT) took center stage in the public debate over electronic voting. Indeed, the debate came to be framed in terms of whether one was for or against the VVPAT.

A VVPAT consists of physical paper records of voter ballots as voters have cast them on an electronic voting system. In the event that an election recount or an audit is called for, the VVPAT provides a supporting record. The "voter-verified" part of the VVPAT refers to the fact that the voter is given the opportunity to verify that the choices indicated on the paper record correspond to the choices that the voter has made in casting the ballot. Thus, the result of an election is an electronic tally of the votes cast and a paper record of the individual votes that have been cast. If all has gone well in the election, the electronic tally and the paper record correspond exactly.

The argument for the VVPAT is based on the fact that in the absence of a physical and enduring record, vote records stored electronically have an inherently uncertain lineage, because a record written fraudulently is indistinguishable from one written legitimately. The concern expressed by advocates of the VVPAT is usually focused on security—that the uncertain lineage of electronic records presents many opportunities for fraud that are not present when nonelectronic voting systems are used. Thus, because the voter himself or herself creates a physical record that can be used if the legitimacy of the electronic tallies is called into question, meaningful recounts and audits become possible that can discern the intent of voters in an election. For a VVPAT to be an effective tool for assuring the integrity of an election, the VVPAT must always be checked against the electronic tally in some voting stations. How many checks are necessary is a statistical sampling issue that depends on the confidence level that election officials require for asserting that no fraud or anomalies within a certain specified error margin have occurred. In the event that this random statistical check suggests that fraud or anom-

Table 3.1 provides a summary comparison of voting technologies in use today.

3.3 THE LARGER CONTEXT

In practice, public debate over electronic voting has devolved into an argument over the technical security of voting systems and whether or not a paper trail to facilitate election auditing is or is not desirable from a public policy perspective. While these issues are important, there are a broad range of end-to-end issues, from the point of capturing the voter's intent to assuring an accurate final tabulation of votes. These issues are themselves embedded in a larger electoral system that

alies may have occurred, or that discrepancies have no reasonable technical explanation, a paper-based recount of all voting stations and/or further investigation may be required.

Some critics of the VVPAT argue that for those elections in which the paper trail is the authoritative record, tallying the vote based on the paper record will entail all of the problems that have plagued paper-based elections over the years. In particular, they argue, there is an ample historical record that documents the vulnerability of paper-based vote counts. Other critics argue that the voter verification dimension of the VVPAT compromises the ability of a blind voter to obtain a secret and independent verification of his or her ballot. Critics also express a variety of concerns about the reliability and additional costs of VVPAT-equipped systems.

In 2001, only two states had a paper ballot requirement. As of this writing (July 2005), a total of 36 states and the District of Columbia have either adopted legislation requiring VVPATs or have such legislation pending. However, whatever one thinks of the arguments for or against a VVPAT, it is indisputable that the debate has been carried out in the absence of substantial empirical data about how a VVPAT would actually work in the context of direct recording electronic systems.

Thus, the impending deployments and expected use of VVPATs in the future provide an important opportunity to test the arguments for and against its use. Some research questions about VVPATs are described in Section 6.8.

NOTE: For arguments that favor the adoption of VVPATs, see David L. Dill, Testimony to the Senate Committee on Rules and Administration, June 21, 2005, Hearing on Voter Verification in the Federal Election Process, available at http://www.verifiedvotingfoundation.org/downloads/Dill%20Statement.pdf. For arguments against the adoption of VVPATs, see League of Women Voters of the United States, *Questions and Answers on Direct Recording Electronic (DRE) Voting Systems and the Proposal to Require a Voter-Verified Paper Trail (VVPT),* available at http://www.lwv.org/join/elections/HAVA_QAonDRE.pdf, and Jim Dickson, *AAPD Policy Statement on Voter Verified Paper Ballots*, available at http://www.aapd.com/dvpmain/elreform/aapdballots.html.

includes matters such as voter registration databases, election planning and administration, procurement of election systems, and so on. Thus, the issue of accuracy of vote counts has to be examined in the context of the entire electoral process. Put differently, challenges to election quality cannot be tied to just one potential problem whose solution would result in a near-perfect election process but rather are the result of the cumulative impact of many potential failures large and small, including human error, equipment snafus, procedural miscues, and so on.

The remainder of this report is devoted to articulating important questions about and related to electronic voting systems in this broader context and explaining why those questions are important.

TABLE 3.1 Comparison of Voting Technologies in Use Today

Method	Percentage of Voters Using	Percentage of Counties/ Towns Using	Name Printed on Ballot?	Tabulation	Error Checking	Central or Precinct Counting	Absentee Ballot Use	Acquisition Cost	Problems
Paper (hand-counted)	<1	9.6	Yes	Manual	None	Depends	Yes	Low	Inefficient and complicated for large numbers of ballots
Punch card	13.7	11.3	No	Computer-assisted	Yes	Precinct	Sometimes	Low	Hanging chad problems
Optical scan	34.9	45.9	Yes	Computer-assisted	Yes	Precinct or central	Yes	Medium	Requires a companion system for voters with disabilities
Lever	14.0	8.5	n/a	Mechanical	Some	Precinct	No	High	No longer manufactured
DRE	29.4	20.0	Yes	Computer-assisted	Yes	Depends	No	High	No direct verification
Other	7.4	4.8							

NOTE: Data presented are for November 2004.

SOURCE: Election Data Services, *Voting Equipment Summary by Type as of 11/02/2004.* Available at http://www.electiondataservices.com/VotingSummary2004_20040805.pdf. A version of this chart was presented to the committee by Eric Fischer, of the Congressional Research Service.

4

Technology Issues

As described in Chapter 1, an election is not a single event but rather a process. It is thus helpful to consider the information technology (IT) of voting in two logically distinct categories: IT for voter registration and IT for voting.

4.1 INFORMATION TECHNOLOGY FOR VOTER REGISTRATION

Voter registration is affected by information technology. Though the subject has received comparatively little attention in the public debate, it is beginning to receive attention. Voter registration is the gatekeeping process that seeks to ensure that only those eligible to vote are indeed allowed to vote when they show up at the polls to cast their votes. Although much of the voter registration process unfolds before Election Day, the final step generally occurs on Election Day. Specifically, citizens register to vote before Election Day, and presuming that they vote at the polls, their voting credentials are checked on Election Day.

Voter registration is a complex process, as one might expect of a decentralized endeavor that involves millions of voters. Historically, voter registration has been a local function, and the primary function of election officials. However, under the Help America Vote Act of 2002 (HAVA), states are required to assume responsibilities that have previously been the province of individual local election jurisdictions. Specifically, HAVA calls for the states to create, for use in federal elections, a "single, uniform,

official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level," containing registration information and a unique identifier for every registered voter in the state. This requirement applies to essentially all states; according to the Department of Justice, this requirement would not be satisfied by local election jurisdictions continuing to maintain their own nonuniform voter registration systems in which records are only periodically exchanged with the state. Rather, HAVA requires a true statewide system that is both uniform in each local election jurisdiction and administered at the state level.[1]

Once a voter registry has been established, two primary technology-related tasks for voter registrars are to keep ineligible individuals off the registration lists and to make sure that eligible ones who are on the lists stay on the lists. A third task—registering new voters—occurs on a regular basis as people come of age or move into a community and want to vote and normally spikes right before or during an election. However, registering new voters occurs on a "retail" case-by-case basis, in contrast to the purging function, which is necessarily done "wholesale."

Purging tasks arise because individuals identified as eligible voters may lose their eligibility for a number of reasons. A list of such reasons from Florida is typical[2] —voters may lose eligibility due to felony convictions, civil court rulings of mental incapacity, death, and inactivity. In addition, a voter may cease to be properly registered, because his or her eligibility to vote in particular electoral contests can be affected by a change in residence or by redistricting that places his or her residence in a different voting district. Finally, an individual registered to vote in more than one local election jurisdiction, even if he or she is otherwise an eligible voter, may vote only in the location in which he or she is legally entitled to vote.

Because lists of registered voters contain millions of entries, the purging of a voter registration list must be at least partially automated. That is, a computer is required to compare a large volume of information received from other secondary sources (e.g., departments of vital statistics for death notices, law enforcement or corrections agencies for felony convictions, departments of tax collection or motor vehicles for recent addresses) against its own database of eligible voters to determine if a given individual continues to be eligible. Note also that states do not in general

[1]See http://www.usdoj.gov/crt/voting/misc/faq.htm.

[2]Florida Department of State, *Florida Voter Registration System: Proposed System Design and Requirements,* January 29, 2004. Available at http://election.dos.state.fl.us/hava/pdf/FVRSSysDesignReq.pdf.

check across state boundaries to see if voters are registered in more than one state or if they have voted in two states on Election Day.

Though this task sounds like a relatively simple one—just compare the lists[3] —it is enormously complicated by two facts: (1) the same individual may be represented on the different lists in different ways (John Jones and John X. Jones may refer to the same person, and he may have given the former name in registering to vote and the latter name in obtaining a driver's license) and (2) the same name (e.g., John Jones) may refer to many different people. (This problem would be greatly ameliorated by the use of an identifier unique to the individual, such as a Social Security number, but for a variety of historical and legal reasons, the nation has chosen to eschew such use.)

Thus, there must be some specific criteria for determining whether or not different names refer to the same person. For example, to deal with the first fact above, one criterion might be this: If similar names have the same home address associated with them, the names refer to the same individual. Such a criterion thus requires a rule for determining "similarity" or a match. One such matching rule might be "if the first and last names are identical, consider the full name a match." Under this approach, John Jones and John X. Jones would be deemed to be the same individual only if they share the same home address, but John Jones and Mary Jones would be deemed different individuals even if they shared the same home address. Suffixes on names, such as Jr. and Sr., can also cause problems in a similar manner.

Similarly, the second fact involving identical names might require a criterion such as, "If the name is associated with several different home addresses, there are as many different individuals as there are home addresses." In this case, the matching criterion applies to home addresses, which are somewhat less ambiguous than names.[4]

The problem of determining whether names match is an algorithmic one. A simple and obvious algorithm calls for a perfect character-by-character match between names. But names in a database may be misspelled (e.g., due to typographical errors), and thus an algorithm that is relatively insensitive to such errors may be of more utility in determining

[3]Lists provided by other sources must also be correct and complete (e.g., all those reported as felons must indeed have been convicted of felonies but not misdemeanors), but that point is outside of the scope of this discussion.

[4]But not entirely. In the District of Columbia, for example, a specific residence may be listed as "3751 Joycelyn Street, NW" and "3751½ Joycelyn Street, NW" in different official records of the D.C. government, depending on whether or not the computer software in use at any given department is able to process "½" as part of a street address.

a match. Names can be pronounced the same way but spelled differently and vice versa. One class of algorithms developed to handle such problems is Soundex algorithms.[5] These algorithms are widely used today for applications involving name matching, and their applications include name matching in comparisons of voter registration databases with other databases.

It is useful to distinguish between a "strong match" and a "weak match." A strong match is one in which there is a very high probability that two data segments represent the same person. A weak match indicates that two data segments are similar, but additional information or research is necessary to determine if the two data segments represent the same person. In addition, there can be many legal ways to identify a citizen who is eligible to vote, which suggests that information in multiple databases can be used to determine eligibility.

Whatever the approach, it is important to realize a trade-off between false negatives and false positives. Any approach will identify some names as different when they do refer to the same individual (false negative) and other names as similar when they do not refer to the same individual (false positive).

Consider the significance of this problem for purging of a voter registration list. Any approach will incorrectly identify some registered voters as ineligible and thus improperly purge them (false positive) and will also fail to find ineligible voters who are not identified as such and thus remain on the list (false negative). For example, John Jones on the voter registration list and Jahn Jones on the convicted felon list may constitute a weak match, and without additional research, John Jones may be improperly removed from the voter registration list (a false positive). On the other hand, the names Sam Smith on the voter registration list and Sam X. Smith on the convicted felon list (with both names referring to the same person) may result in Sam Smith improperly remaining on the voter registration list (a false negative).

It is a fundamental reality that the rate of false positives and the rate of false negatives cannot be driven to zero simultaneously. The more demanding the criteria for a match, the fewer matches will be made. Conversely, the less demanding the match, the more matches will be

[5]Soundex algorithms solve the generic problem of matching names that sound alike but have different representations in text form (e.g., Smith and Smithe). A Soundex algorithm generates a string of characters that represent approximately its phonetic sound, so that words that sound alike, even if spelled differently, all result in the same character string when proceeding through the algorithm. The original Soundex algorithm was patented in 1918, and there have been refinements to it over the years, resulting in a class of such algorithms.

made. For example, a requirement that names match (using all of the letters), addresses match, and dates of birth match is more demanding and will result in fewer matches than if the requirement is that only names and addresses match and only some of the letters and/or sounds in the name are used to determine a match. The choice of criteria for determining similarity is thus an important policy decision, even though it looks like a purely technical decision.

Furthermore, the considerations discussed above suggest that the presence or absence of human intervention in the purging process is important. That is, one should regard as very different a purging system that is fully automated and one that uses technology only to flag possible individuals for further attention by some responsible human decision maker. Because the human decision maker would use different criteria to render a decision (including the use of common sense and contextual factors), the rate of false positives would be reduced—and considerably so if the different criteria could be applied consistently.

In addition, the use of lists of inactive voters can provide some protection against false positives. A purge removes a voter from the voter registration list entirely, and thus this voter would either be denied the ability to vote or might be allowed to cast a provisional ballot. But if a voter who might otherwise have been purged is moved instead to an inactive voter list, the voter still remains on the rolls—and may vote in a subsequent election.

Finally, the purging of voter registration lists must itself be seen in a larger context, as such purging can be used as a political tool to manipulate the outcome of elections. One such use is to purge in local election jurisdictions chosen so that a purge would have differential effects on various voting blocs. Statewide management of voter registration lists reduces the possibility that decisions to purge are made locally, but there may be nothing in state law that in principle or in practice prevents state officials from ordering such purges for political reasons.

The issue above is important because there must be some criterion by which to determine if a purging is undertaken overaggressively or underaggressively. An overaggressive purge purges individuals who should be retained on the rolls. An underaggressive purge does not purge individuals who should not be retained on the rolls. Either type of purge can be undertaken for political reasons, depending on the demographics of those inappropriately retained on or purged from the rolls.

One approach to understanding the nature of a purge is to compare the rate at which eligible voters are inappropriately purged (E) with the rate at which ineligible voters are not purged (I). That is, define R as the ratio of I to E. Thus, R reflects the number of ineligible voters who are not purged for every eligible voter who is purged. Those who put a very high

premium on eligible voters not being purged want *E* to be as low as possible, and thus tend to favor large *R*. Those who put a very high premium on purging the voter rolls of all ineligible voters want *I* to be as small as possible, and thus tend to favor small *R*.

In any event, given a certain fraction of ineligible voters in the voter registration database, the choice of *R* determines a great deal about the performance requirements of the purging process. As Box 4.1 illustrates, the choice of *R* fixes the relative effectiveness of the purging process in identifying eligible voters for retention compared with not identifying ineligible voters for purging.

Note also that Election Day credential checking involves a similar set of considerations. A citizen presents his or her credentials at the polling place, and these credentials are checked against a listing of eligible voters. Again, the issue of similarity is relevant. If the eligibility credential is an excerpt from the voter registration database (e.g., a voter registration card), the possibilities for error are minimized. But if, instead, the requirement is to prove one's identity with some other set of credentials, such as a driver's license, a judgment of similarity must again be made. However, this time the criteria—which may or may not be the same as those used for purging voter registration lists—work in the opposite direction. A demanding similarity criterion will tend to exclude eligible voters, while a less demanding criterion will allow more ineligible individuals to vote (or at least result in more confusion between different individuals).

Against the discussion above, a number of important questions arise:

4-1. **Are the relative priorities of election officials in the purging of voter registration databases acceptable?** As noted above, purging databases can be conducted in an overaggressive manner or in an underaggressive manner. The politically correct response for public consumption is that it is equally important to purge the registration rolls of ineligible voters and to ensure that no eligible voters are purged, but of course in practice officials must choose the side on which they would prefer to err. An explicit statement of *R*—the number of ineligible voters who are not purged for every eligible voter who is purged—is thus a quantitative measure of the direction in which a given policy is leaning. (Of course, being able to make an estimate of *R* requires that data be collected that indicate the probability that an eligible voter on the voter registration rolls is wrongly purged, the probability that an ineligible voter on the voter registration rolls fails to be purged, and the fraction of the voter registration rolls that actually consists of ineligible voters.)

4-2. **What standards of accuracy should govern voter registration databases?** In voting machines, a Federal Voting Systems Standard specifies a maximum error rate of 1 in 500,000 voting positions (e.g., 1 in every

Box 4.1
False Positives and False Negatives

Let P_{fp} = the probability that an eligible voter on the voter registration (VR) rolls is wrongly purged.

Let P_{fn} = the probability that an ineligible voter on the VR rolls fails to be purged.

Let f = the fraction of the VR rolls that actually consists of ineligible voters.

Each cell entry in the table below indicates the probability of the action taken given the status of an individual on the VR roll. In the ideal case (a perfect algorithm), the likelihood of purging an eligible individual is zero, as is the likelihood of not purging an ineligible individual.

	Status of Person on VR Roll	
Action Taken	Eligible	Ineligible
Not purged	1	0
Purged	0	1

In the more realistic case, with nonzero P_{fp} and P_{fn}, the probabilities are as follows:

	Status of Person on VR Roll	
Action Taken	Eligible	Ineligible
Not purged	$1 - P_{fp}$	P_{fn}
Purged	P_{fp}	$1 - P_{fn}$

By definition, f is the fraction of the database of size N that consists of ineligible individuals. Based on the tables above, the cell entries below indicate the number of people who are eligible (ineligible) who are subsequently purged or not purged.

	Number of Individuals on Roll Who Are	
Action Taken	Eligible	Ineligible
Not purged	$(1 - P_{fp})(1 - f)\ N$	$P_{fn}\ fN$
Purged	$P_{fp}(1 - f)\ N$	$(1 - P_{fn})fN$

If we define R as

$$R = \frac{\text{Number of ineligible individuals who are not purged}}{\text{Number of eligible individuals who are purged}}$$

then

$$R = \frac{P_{fn}\ fN}{P_{fp}\ (1 - f)\ N}.$$

2,000 punch card ballots with 250 voting positions on each card). What might be a comparable standard for the accuracy of a voter registration database, taking into account that people move frequently and die eventually?

4-3. **How well do voter registration databases perform?** How many people who think they are registered really are registered? How many people who are registered should be registered? The first question requires a general population survey that is linked to registration records (the American National Election Studies did this for many years). The second question requires a sample from the registration list followed up with diligent efforts to contact the people and the collection of information about them.

4-4. **What is the impact on voter registration database maintenance of inaccuracies in secondary databases?** The quality of databases other than those for voter registration affects maintenance of voter registration databases. In general, databases such as those of departments of motor vehicles (DMVs), departments of correction, and departments of vital statistics are not under the control of the state election officials. (Vital statistics are usually under the control of a county or municipality.) For example, if a DMV database is highly inaccurate in its recording of addresses, and a decision on voter eligibility depends on a match between the address on the voter registration database and that of the DMV, the probability of purging an eligible voter increases, all else being equal. A related point is the fact that database interoperability is in general a nontrivial technical task. The secondary databases needed for verification of voter registration are developed for entirely different purposes, and both the syntax and semantics of those databases are likely to be different from those of the voter registration databases.

Finally, these secondary databases are subject to state legislative control as well, and there are a wide range of options for how legislatures can affect their disposition and use in the voter registration process. For example, states could explicitly disclose these sources, so that a voter could be especially careful to ensure that he or she is not being misrepresented in such databases. States could mandate that secondary databases be managed with a higher level of care when they are used for purposes related to voter registration. Or states could mandate that in the interests of protecting voter privacy only certain types of data in these secondary databases would be available to the voter registration process. More generally, refining criteria for the various legal reasons for purges has been and will be on the agenda of many legislatures, and discretion based in local election jurisdictions about how to conduct purges will probably be subject to increased scrutiny.

4-5. **Will individuals purged from voter registration lists be notified in enough time so that they can correct any errors made, and will**

they be provided with an easy and convenient process for correcting mistakes or making appeals? From the discussion above, it is clear that some number of eligible voters will be inappropriately purged in any large-scale operation. Given that the right to vote is a precious one, voters who may have been purged incorrectly should have the opportunity to correct such mistakes before they cast their votes.[6]

4-6. **How can the public have confidence that software applications for voter registration are functioning appropriately?** As the discussion in Section 4.2.1 indicates, software for voting systems is subject to a variety of certification and testing requirements that are intended to attest to its quality. But there are no such standards or requirements for software associated with voter registration. Voters who lack confidence in the operation of voter registration systems will be uncertain about their ability to vote on election day. Large numbers of such voters will almost surely result in reduced turnouts.

4-7. **How are privacy issues handled in a voter registration database?** In many states, much of the information in a voter registration database is public information. HAVA directs states to coordinate those databases with drivers' license databases of state DMVs and with the U.S. Social Security Administration. States may choose to coordinate with other databases as well, such as databases containing identification information for felons and death records. Much of the information in these other databases is not relevant to one's eligibility. For example, one's driving record is contained in a database of licensed drivers maintained by the state DMV. This database may be used to verify names and addresses for voter registration purposes (checking consistency, for example), but one's driving record is not relevant for determination of voting eligibility. How do state laws, regulations, or guidelines limit the fields that constitute public information or the extent to which the interfacing agencies are permitted to retain personal data received from the other agencies during the matching process required for voter registration? How, if at all, is such nonrelevant information protected from inappropriate disclosure? How might such nonrelevant information be used to bias voter turnout for partisan

[6]Provisional balloting is a method required by HAVA that enables provisional ballots to be cast, subject to subsequent validation of a voter's credentials. Though in principle such an approach solves the problem of an improperly purged voter, there are two potential problems with it. First, for all practical purposes, a provisional ballot has the same privacy protections as an absentee ballot—which are necessarily of a lesser degree than the privacy protections available in the voting booth on Election Day. Second, provisional ballots are inherently suspect in a way that votes cast in a voting booth are not, and the voter casting a provisional ballot will leave the polling place without any assurance that the ballot will indeed be counted.

purposes? (Indeed, much of the information contained in these databases is for sale by the states, and the purchasers of such information are often political parties.)

4-8. **How can technology be used to mitigate negative aspects of a voter's experience on Election Day?** For example, in many large jurisdictions, check-in lines at polling places can be both long and uneven. One frequently heard reason for this phenomenon is that any given poll worker checking registration can only check certain last names (e.g., all those names starting with letters A through G). This is true because the roll books containing lists of registered voters are broken up that way, and the poll workers have no flexibility on this point. However, information technology might be used to provide such similar information to poll workers without the need for such a procedure.[7]

4-9. **How should voter registration systems connect to electronic voting systems, if at all?** Today, there is an "air gap" between voting, even if done electronically, and checking for voter registration, which is done manually. However, in the interests of efficiency and rapid movement through polling places, it is easy to see a persuasive argument for why these functions should be integrated. A voter could simply present an electronic registration card to a voting station and be allowed to cast a ballot. This arrangement might facilitate easy, vote-anywhere voting in thousands of locations across a state rather than in just one precinct location and also early voting, in which a voter could vote at a central site. In both situations, a voter could have high assurance that he/she received the correct ballot form corresponding to his or her registration address. The most obvious argument against this arrangement is that it potentially compromises the secrecy of voting in a major way. Nevertheless, it is easy to imagine that both voter registration and voting might be integrated in packages of services offered by election service vendors.

4.2 INFORMATION TECHNOLOGY FOR VOTING

IT for balloting is what is usually meant by "electronic voting systems"—the systems described in Chapter 3. This section addresses security and usability issues. Usability can be characterized as functionality that facilitates a voting system's accurate capture of a voter's intent in casting a ballot and assures the voter that his or her ballot has been so captured. Furthermore, the voting system must record that ballot accu-

[7]This is not to say that the use of information technology for this purpose has no downsides. For example, it may be more difficult to capture a signature if one is required.

rately until it is tabulated, even in the face of deliberate wrongdoing (security) or accidental error or mishap (reliability).

4.2.1 Approaching the Acquisition Process

In considering the purchase of any given voting system, an election official's first step is often to consider systems that have been qualified under a process established by the Election Assistance Commission (EAC). Specifically, a vendor's voting system is qualified if an Independent Testing Authority (ITA) asserts that the system in question meets or exceeds the Federal Elections Commission's 2002 Voting Systems Standards (Box 4.2).[8] ITAs are designated by the National Association of State Election Directors, and a vendor pays an ITA for its work in qualifying a system.

Knowledge that a given voting system has been qualified according to a particular standard provides some degree of assurance that the system in question meets a minimum set of requirements. Nevertheless, the fact that a given voting system has been qualified may not be the only criterion that affects a decision maker's procurement decision.[9] This is because voting systems fit into a larger context that cannot be separated from an assessment of fitness for purpose. The election official is responsible for the conduct of an election with integrity, and the equipment used in the election is only one part of that election. Yet, the qualification process evaluates voting systems, making just such a separation. This is not the fault of the qualification process—it is simply a consequence of the fact that any testing process must necessarily set bounds on the scope of the evaluation.

Of particular significance is the fact that various jurisdictions have long-established policies, procedures, and practices that govern the conduct of elections. Introduction of new technology into established practices almost always results in some degree of conflict and difficulty, even when the authorities seek to adjust existing practices to accommodate the new technology. Technology may work properly only if certain pro-

[8]The Federal Election Commission's 2002 Voting Systems Standards call for three kinds of tests to be performed on voting systems to ensure that the end product works accurately, reliably, and appropriately: qualification testing (the focus of this section), certification tests performed by states in order to document conformance to state law and practice, and acceptance tests performed by the jurisdiction acquiring the system to document conformance of the delivered system to characteristics specified in the procurement documentation as well as those demonstrated in the qualification and certification tests.

[9]In practice, qualification may only be a prerequisite for a vendor to be considered for purchase. That is, a county may be interested in "all qualified systems"; thus, the fact of qualification may have no relationship to a specific purchase decision.

Box 4.2
Federal Voting Systems Standards

To address some of the difficulties of technology assessment for state and local election officials, the Election Assistance Commission (EAC) has responsibility, with assistance from the National Institute of Standards and Technology (NIST), for developing voluntary standards that help to provide assurance that conforming voting systems are accurate, reliable, and dependable. Initially approved by the Federal Election Commission (FEC) in 1990, with a revised edition released on April 30, 2002, these standards are again being revised as this report goes to press.

The FEC 2002 Voting Systems Standards (VSS) cover functional capabilities required of a voting system—what a voting system is required to do—but not election procedures or report formats. The functional capabilities include (1) a set applicable to all parts of the election process, including security, accuracy, integrity, system auditability, election management system, vote tabulation, ballot counters, telecommunications, and data retention; (2) prevoting capabilities, used to prepare the voting system for voting, such as ballot preparation; (3) voting capabilities, such as the casting of ballots at the polling place by voters; (4) postvoting capabilities that are relevant after all votes have been cast, such as obtaining reports for individual voting machines, polling places, and precincts; and (5) maintenance, transportation, and storage capabilities relevant to voting system equipment.

In addition, the FEC 2002 VSS cover hardware standards for performance, physical characteristics, and design; software standards intended to ensure that the overall objectives of accuracy, logical correctness, privacy, system integrity, and reliability are achieved; telecommunications standards that govern the capability to transmit and receive data electronically (e.g., via modem); security standards intended to achieve acceptable levels of integrity, reliability, and inviolability in conforming systems; standards for quality assurance such as documentation of the software development process; and standards for configuration management of voting systems.

In April 2005, the EAC's Technical Guidelines Development Committee released a first draft of technical guidelines that add to the FEC 2002 VSS in the areas of security and transparency of voting systems, usability of voting systems, and core requirements and testing. After a period of comment, it is expected that the EAC will promulgate the augmented Voluntary Voting System Guidelines (VVSG)—Version 1 as the first round of a new set of standards. A second round of review for all of the VVSG is expected to follow, resulting in an integrated and forward-looking version of the VVSG that should be available in FY 2006.

cedures are followed by poll workers, for example, and any given set of standards may—or may not—presume that these procedures are followed.

Moreover, the qualification process may not be adequate for a particular jurisdiction's needs. For example, an election official from a jurisdiction with a long history of fraud and corruption may perceive security

issues in a different light than an administrator from another jurisdiction without such a history. For the former, a given set of security standards may be inadequate, but for the latter, the same set may be more than adequate.

An important technical point is that the voting stations deployed in a particular jurisdiction may not be identical. A great deal of hard-earned experience in the IT world suggests that a station running software version A may work perfectly with other stations running software version A, and a station running software version B may work perfectly with other stations running software version B, but that a station running software version A is unreliable when it connects to a station running software version B. Or, a station may be secure when in stand-alone operation but much less secure when connected to a network.

Similar points apply to hardware and software qualification. The same body of experience suggests that especially when custom hardware is involved (as it is for nearly all voting systems), it is the total package—software of a specific version running on hardware of a specific model—that must be evaluated. And, a small change to a qualified piece of software can in principle render it noncompliant with the relevant standards.

For such reasons, election officials may wish to go beyond the qualification process in their assessments of vendor offerings. The discussion below focuses on two areas of particular significance: security and usability/accessibility.

4.2.2 Security

4.2.2.1 Perspectives on Security

A very important requirement of any information technology deployed in a critical application is that it be secure and reliable. Security involves its resistance to deliberate acts of fraud that cause the system to record votes differently from what was intended by the voters who cast them.[10] Thus, a voting system must ensure that ballots are counted as cast and that the resulting vote counts are accurate, despite malicious hacker attacks or insiders hired or planted to alter election results. (The system must also be reliable—that is, resistant to unplanned events that

[10]In the computer science community, the term "security" (or "computer security" or "information security") is often used to denote a broader set of concerns, including integrity (e.g., being able to prove that a message has not been altered) and confidentiality (e.g., keeping the contents of a message private to unauthorized parties). In the present context, the term "integrity" as used by computer scientists more accurately describes the inability to alter a vote once it has been cast. However, in the debate over electronic voting systems, the term "security" has been used instead, and that term is adopted for this report.

render it unavailable for normal use by voters; such events include power failures, unanticipated input sequences that might cause the system to freeze, accidentally introduced software bugs, and potential administrative mishaps or errors. These are not security issues per se and are not addressed further in this report.)

Moreover, in the electoral context, the public must have reason to believe in the security of the system, even in the face of those inclined to challenge it. That is, even if a system is in fact robust against such problems, perceptions of a system's security depend on people's experience with those systems, media exposure, and public debate. With new technologies being frequently deployed, election officials may face the task of assuring the public that the new systems are in fact secure and reliable, even if no problems arise immediately. At the same time, the consequences of inaccuracy and/or system failure place election officials on the front line of responsibility that could ultimately affect the outcome of any election. This point is particularly relevant given the discussion in Chapter 2 about a polarized electorate.

Security issues in voting are among the most difficult that arise in the development of secure systems for any application. Systems to manage financial transactions, for example, must also be highly secure, and much of the experience and knowledge needed to develop secure systems for financial applications is directly relevant to the development of secure systems for voting. But these applications differ from voting applications in at least two important ways.

First is the need to protect a voter's right to cast a secret ballot. Developing an audit procedure (and the technology to support audits) is enormously more difficult when the transactions of an individual must not be traceable to that individual. (Consider, for example, the difficulties in reconciling accounts if it were by design impossible to associate an individual with the amount of a specific transaction.)

Second, under many circumstances, the value of security in financial systems can be quantified as just another cost-benefit trade-off. For those instances in which it is possible to estimate the likelihood of a particular kind of security breach, it is possible to compare the cost of securing that breach to the expected loss if the breach is not secured. Such a cost-benefit analysis is difficult for voting applications, because there is no commonly accepted metric by which one can quantify the "value" of a vote. Thus, an advocate of one position might argue that the relevant point of comparison for the security of voting systems should be the nuclear command-and-control system, while another might argue that commercial banking security is the appropriate comparison.

Also, election systems must declare a winner even when the margin of victory is minuscule. When the vote is close, a very small number of

votes can sway the election one way or another. Thus, in closely contested races, an election fraudster must manipulate only a small number of votes in order to obtain the desired outcome—and small manipulations are almost invariably more difficult to detect than large ones.

From the perspective of the computer scientist, security is a particularly elusive goal. Except in very rare instances that are for practical purposes not relevant to complex systems (and electronic voting systems count as complex systems), it is impossible to achieve 100 percent security in a system. Even worse, it is impossible to specify in any precise way what it would mean for a system to be 99 percent or 90 percent secure.

To illustrate, system testing is a process that is used to identify defects in a system (e.g., security vulnerabilities, software bugs). A vulnerability or a bug is detected when there is evidence that indicates its presence. But because the conditions under which a complex system can operate are so varied, no reasonable amount of testing can prove that the system is free of vulnerabilities or bugs. Moreover, the fixing of a particular system vulnerability takes place in the context of a would-be attacker who is motivated to continuously explore a system for such vulnerabilities. This implies that system security must also be a continuous and ongoing process that searches for vulnerabilities proactively and fixes them immediately.

A key point about security is that a system is only as strong as its weakest link. System security is a holistic problem, in which technological, managerial, organizational, regulatory, economic, and social aspects interact,[11] and the attacker's search for vulnerabilities is not limited to technological vulnerabilities. The technological security provided to pre-World War II France by the Maginot Line was high—but German tanks circumvented the line. In an election context, it makes little sense to enhance security in particular areas (e.g., in the computer-related parts of the election system) if enormous vulnerabilities remain in the other parts of the system whose exploitation could be problematic. At the same time, security in particular areas has to be compared by asking how much damage an adversary can do with a given amount of effort and a given risk of discovery. That is, gaping security holes in one part of the system (e.g., the noncomputer part) may be of lesser concern than smaller security holes in another part of the system if the latter can be exploited on a large scale more easily and more anonymously.

Cybersecurity experience suggests that there is only one meaningful technique by which the operational security of a system can be assessed: an independent red team attack.[12] The term refers to tests conducted by

[11]National Research Council, *Cybersecurity Today and Tomorrow, Pay Now or Pay Later*, Washington, D.C.: National Academy Press, 2002.

[12]NRC, *Cybersecurity Today and Tomorrow*, 2002.

independent groups, often known as "red teams" or "tiger teams," that probe the security of a system in order to exploit security flaws just as they would be uncovered by a committed attacker in an actual attack.[13] Flaws are then reported to the party or parties who hired the red team. Vendors sometimes use red teams as a way of improving their products, while customers sometimes use red teams as a way of assessing the security present in a product they may buy or have bought. Conducted properly, a red team attack does whatever is necessary to compromise the security of a system, exploiting technological or procedural flaws in the system's security posture or flaws in the human infrastructure in which the technology is embedded. (A technological flaw might be the use of a weak encryption algorithm. A procedural flaw might be a poll worker who can be bribed to take an improper action.) Red team attacks are also unpredictable, in contrast to scripted tests in which the system's developer tests what it believes to be likely attacks.

As a general rule, many computer scientists are also skeptical of "security by obscurity," a practice that involves hiding vulnerabilities rather than fixing them. The reason is that information about vulnerabilities, especially those of high-value systems, is enormously difficult to keep secret. Moreover, such vulnerabilities are often discoverable through the application of enough technical expertise and experimentation. Open discussion of vulnerabilities, argue these individuals, provides strong incentives for system owners to fix them or to configure their systems in such a way that hostile exploitation of the vulnerabilities is less (or not) harmful.[14]

For such a strategy to be meaningful, the source code of the system in question must be available for inspection, because it is the code actually running on the system that defines its behavior under all possible circumstances. Without access to source code, it would be essentially impossible to discover, for example, that the system is programmed to behave in one way until a specific sequence of keys is pressed with the right timing between key presses, at which time the system's behavior shifts into an entirely different mode that allows access to and manipulation of the data

[13]To date, red team attacks against electronic voting systems have not been undertaken under conditions that resemble the actual use of voting systems in the field.

[14]To be more precise about this argument, obscurity (concealing the internal workings of a system) can and does provide a layer of protection for a system. But there are many disadvantages to relying only or primarily on security by obscurity of the sort described above, and these disadvantages may well (and often do) outweigh the advantages provided by obscurity. At the same time, good security design and implementation can reduce those disadvantages—a point well recognized by the National Security Agency's classification of many encryption algorithms.

contained within the system. Indeed, such practices are common in software developers, who often install such "back doors," known as maintenance traps, to facilitate system maintenance and debugging. While traps are a convenience for system developers, they are also blatant security holes and as such should not be included in production versions of the software. Alas, the pressures of software development under deadline are such that they are often included in production versions anyway.

When approaching any computer security problem, the computer scientist's perspective can be summarized as a worst-case perspective—if a vulnerability cannot be ruled out, it is necessarily of concern. Furthermore, the computer scientist argues, a wealth of experience suggests that even obscure vulnerabilities in a system can be and often are exploited to the detriment of the system owner.

Computer scientists also note that the use of computers in voting makes possible the commission of automated fraud. Throughout most of the history of voting, the magnitude of fraud was strongly dependent on the number of people or on the effort required to commit fraudulent acts such as stuffing ballot boxes—larger numbers of fraudulent votes required a larger number of people. However, when computers are involved, a small number of individuals—albeit technically sophisticated individuals with high degrees of access to the internals of these computers—become capable of committing fraud on a very large scale indeed. Furthermore, because the software of computer systems is intangible, the difficulty of detecting such attempts is greatly increased.

It is thus not surprising that these perspectives shape the way that computer scientists look at security issues in electronic voting systems. In the words of one computer scientist:

> As a general rule, the burden and cost should be on advocates of a particular voting product to provide evidence to the panel that the product is safe, rather than on critics to prove to the panel that it is unsafe. In case of doubt, a voting system should be considered unsafe until proven safe, and election officials should refrain from certifying, purchasing, or deploying voting equipment until independent security reviewers are confident that the technology will function as desired.[15]

The perspective of the election official is quite different. From a public policy perspective, it is desirable for election officials to have open attitudes about election concerns raised by members of the public, to welcome skepticism as a way of reassuring the public about how elections are conducted, to treat every election as precious, and to strive to eliminate

[15]David Wagner, University of California, Berkeley.

Box 4.3
Burdens of Proof

As a matter of public policy, many states have adopted legal frameworks to promote a high degree of scrutiny for documents and processes related to the operation of government. According to this freedom-of-information philosophy, information related to the operation of government must be available to the public unless specifically exempted by law—the essential notion being that the making of public policy should itself be public.

Against this standard, every aspect of the election process, including records, procedures, and vote-counting mechanisms, ought to be subject to public inspection. However, in practice, the convergence of several issues has attenuated the degree to which such inspection is possible. Vendors have asserted intellectual property rights in order to keep the source code of electronic voting systems out of public view (and most freedom-of-information laws specifically exempt proprietary information from disclosure)—a point of controversy in the public debate. The short period available to election officials for declaring a winner means that the time available for public inspection and access is short. And, the political pressures from all sides in an election to know its outcome rapidly mean that election officials have strong incentives to avoid recounts that might delay the declaration of a winner.[1]

If election processes—and in particular, source code—were available for inspection, critics of electronic voting systems could reasonably be expected to assume the burden of demonstrating that security problems exist. But because such information is not available, these critics become "outsiders" to the election process and thus must use the tools available to outsiders—public discussion of potential vulnerabilities, close scrutiny of election events, and media attention—to draw attention to the issues they raise.

[1]In addition, election officials who are attempting to maintain or to create partisan advantage have incentives to avoid recounts that might reduce or eliminate their advantage.

every possibility of error. Indeed, election officials are responsible for the safety and security of an election, and as a rule, they accept that the burden of assurance properly rests on their shoulders (Box 4.3).

But in practice, resource constraints, time pressures, the lack of administrative control, and simple mistakes make the normative goals described in the previous paragraph difficult if not impossible to achieve. How election officials actually behave ranges from idealistic to pragmatic (and in some—hopefully rare—cases, politically expedient or partisan as well).

There is also the point that the victors in an election are—by definition—transient. The preservation of democracy has historically depended much more on the integrity of elections taken over time than it does on the outcome of any single election. In the more than 200-year history of the nation, there have been hundreds of thousands of electoral contests,

and despite more than occasional fraud or irregularity in elections, the democracy endures—at least in part because election officials have taken measures to fix the problems that allowed those problems to occur.

Election officials also have multiple goals. Sharon Priest, once secretary of state for Arkansas and a former president of the National Association of Secretaries of State, notes that most election officials are necessarily as concerned with affordability, system usability, turnout, and compliance with the federal, state, and local laws that govern elections as they are with security—which suggests that security is not the only, sole, or primary issue for them, but rather is one of several equally important issues.

Indeed, election officials have learned over the years that misfeasance is typically a greater risk than malfeasance. That is, election workers routinely make mistakes and technologies routinely fail without obvious partisan bias. Ballots are lost, procedures are not followed, and improvised solutions are put into place to respond to pressures of the moment on Election Day. Although the impacts of misfeasance are likely to be more or less random, they still account for the majority of obvious problems that election officials must address with limited resources. And, as a result, administrators have generally paid more attention to improving the procedures that have led to such problems than to improving technology.

From the point of voter registration to the moment of winner certification, there are many opportunities for something to go wrong—both deliberately and accidentally—that can potentially affect an election outcome. As with all public officials, election officials do not have the resources to deal with all problems, and they necessarily leave some unaddressed. Within the constraints of their limited resources, they must set priorities—and their perceptions of the likelihood of various problems play an important role in setting those priorities. If it can be shown that a set of events has actually affected the outcome or tallies of an election, it is inevitable that an administrator will believe the likelihood of that kind of problem is greater than the likelihood of other sets of events that have not yet affected outcomes or tallies.

While political loyalties can and do protect the tenure of some election officials, other election officials realize they can lose their jobs if an election is not carried off correctly. Elections still must be decided, even when races are close. Close races increase the likelihood of recounts, and recounts dramatically increase the likelihood of vulnerabilities being exposed. For understandable reasons, many election officials would prefer to avoid such careful scrutiny.

Consider how these different perspectives play out in the consideration of election fraud. Election fraud, or the appearance of fraud or impropriety, can undermine public confidence in elections. But, of course,

the nondetection of fraud, whether in traditional or electronic voting systems, can mean either that there has been no fraud or that the fraud was successfully concealed—and there is no a priori way of determining which of these is true. That is, although some statistical techniques can suggest that fraud may have been committed,[16] these techniques are based largely on historical data, and their indications do not come anywhere near a legal standard for asserting that fraud has occurred. In short, no one knows the baseline level of fraud in elections, regardless of what technologies have been used,[17] and because there are many impediments to conducting recounts (especially in high-profile races),[18] it is unlikely that fraud—if it exists—will be discovered.

Election officials and legislators tend to respond to fraud cases that have come to light during their tenure. By this standard, some election officials are skeptical of the claim that electronic voting systems without paper trails are less secure than nonelectronic systems, partly because most proven instances of election fraud to date have involved nonelectronic voting systems.[19] And, in response to the possibility of fraud, many election officials have worked to improve procedures and organization that enhance the overall security posture of elections.

On the other hand, electronic voting systems have not been in use for very long, and so it may simply be that election irregularities and fraud associated with these systems have not yet come to light. By contrast, computer scientists see myriad possibilities for fraud, and because there is no way to rule out those possibilities or to bring them to light, they tend to behave as though such possibilities must be taken for granted. Moreover, they are concerned that the use of electronic technology enables the

---

[16]See, for example, Jonathan N. Wand et al., "The Butterfly Did It: The Aberrant Vote for Buchanan in Palm Beach County, Florida," *American Political Science Review* 95(4): 793-810, 2001.

[17]See, for example, Fabrice Lehoucq, "Electoral Fraud: Causes, Types, and Consequences," *Annual Reviews of Political Science* 6:233-256, 2003; Larry Sabato and Glenn Simpson, *Dirty Little Secrets: The Persistence of Corruption in American Politics*, New York, N.Y.: Random House/Times Books, 1996; John Fund, *Stealing Elections: How Voter Fraud Threatens Our Democracy*, San Francisco, Calif.: Encounter Books, 2004.

[18]Such impediments include the high cost of recounts and the fact that a winning candidate is virtually certain to oppose a recount using any legal mechanism available—and there are many such mechanisms.

[19]Dozens of problems with electronic voting systems have been documented, and allegations of fraud involving electronic voting have appeared in the form of signed affidavits. Testifying before the U.S. House of Representatives Committee on House Administration, July 7, 2004, Michael Shamos reported that since 1852, the *New York Times* has published over 4,000 articles detailing numerous methods of altering the results of elections through physical manipulation of ballots (available at http://euro.ecom.cmu.edu/people/faculty/mshamos/ShamosTestimony.htm).

commission of fraud in ways much more subtle than in the past and that these technology-enabled frauds may be much more difficult to detect.

Whereas computer scientists often compare what they have today with what could be in principle, administrators tend to compare what they have today with what they had yesterday. Computer scientists will presume a vulnerability is significant until shown otherwise, but election officials will presume that the integrity of an election has not been breached until compelling evidence is produced to the contrary. This difference in perspective largely accounts for the tendency of some election officials to blame electronic voting skeptics for scaring the public about security issues and for the tendency of some electronic voting skeptics to say that election officials have their heads in the sand.

As a baseline for comparison purposes, consider the security of a voting system based on hand-counted paper ballots. Such a system is manifestly subject to fraud if the chain of custody is not well defined or maintained, as the expression "stuffing the ballot box" indicates. Fraudulent votes can be introduced through the counterfeiting and subsequent marking of ballot documents, and while there are techniques that can be used to authenticate a document as legitimate, they all require that ballot documents be checked one by one. All else being equal, manual (re)counting of ballot documents is relatively straightforward when the number of voters involved is small, but it becomes more prone to error when hundreds of thousands of ballots are being recounted.

It is helpful to categorize security questions according to the timeline of a system's use.[20] First, a system (including all necessary hardware and software) should be assessed for its security. Second, if the system's security is found adequate, the assessed system must be propagated to all the sites where it will be used. That is, the physical units that voters actually use should be identical to the system that was assessed. A third set of security issues arises while the systems are being operated by the voters. The fourth and final set of issues arises after the polls close and the results of each unit are passed to the parties responsible for vote tabulation.

4.2.2.2 Assessing the Security of a System Prior to Deployment

It is broadly accepted that independent testing and evaluation are an essential component of assessing the security of a system, and at this writing, the EAC is in the process of establishing Voluntary Voting System Guidelines (VVSG) in the area of security. Box 4.4 describes some of

[20]Testing issues are discussed in Douglas Jones, *Testing Voting Systems*, available at http://www.cs.uiowa.edu/~jones/voting/testing.shtml.

Box 4.4
Security Issues That an Independent Assessment Might Examine

An assessment of the security of a voting system would involve independent technical experts with backgrounds in computer security and the ability to draw on people with deep knowledge of election practices and procedures. The assessment team should control the process, and it should have full access to all system documentation, software, source code, change logs, manuals, procedures, training documents, all material provided to any other testing or review process, and working physical examples of the voting system in question (hardware and software). In addition, the assessment team must have adequate resources and time to complete its assessment, and it must have the independence to make its findings known without intervention on the vendor's part.

Assessments of this nature include but are not limited to finding specific software problems. They are intended to examine the system holistically to determine the extent to which it will be capable of resisting attempts to compromise its security (for example, how resistant is the system to the bribing of a single insider?). Collectively, the group responsible for assessing security might examine:

Hardware

- Accessibility of data- or processing-related components internal to a voting station
- Detectability of attempts to tamper with internal components
- Configuration and programming of firmware and any boot-related devices or media

the issues that an independent laboratory might consider in such an assessment.

Security vulnerabilities introduced into an electronic voting system prior to its deployment are the most serious in terms of their potential impact on the outcomes of elections.[21] The reason is that vulnerabilities built into the design of a system are propagated to every individual unit. Thus, the design and implementation phase of system development is a

[21]Note that an explicit evaluation of the security of a specific electronic voting system is not the only possible approach to making electronic voting credibly secure. Whereas an explicit evaluation seeks to uncover security flaws that might exist in any given implementation, a redundant implementation—that is, a competing implementation sponsored and created by any political party with a stake in elections—would require that at least two independent systems be compromised in order to commit fraud successfully. However, the redundant approach has not been adopted for electronic voting, though it has been used in a variety of situations where high reliability and security are required.

- Ability to reprogram boot sequences
- Ability to access ports remotely

Software

- Source code inspection and verification
- Logic and accuracy testing
- Ability to ensure that code is digitally signed
- Security features built into the software (e.g., authentication protection for access to system internals)
- Reliability (e.g., ability to recover from a power failure)
- Architecture and design for modular construction
- System behavior under different configurations (e.g., different ballots, ballots for people of different abilities)
- Maintenance "traps" that circumvent normal protections.

Procedures

- Procedures for upgrading or patching software
- Procedures for qualifying and certifying patches (or, in fact, the system configuration after a patch has been installed)
- Procedures for decertifying or dequalifying software or hardware
- Procedures for setting up and breaking down the system in operational use
- Procedures for handling vote totals at the close of the polling place

SOURCE: Drawn in part from Leadership Conference on Civil Rights and the Brennan Center for Justice, New York University, *Recommendations for Improving Reliability of Direct Recording Electronic Voting Systems*, June 2004. Available at http://www.civilrights.org/issues/voting/lccr_brennan_report.pdf.

point of high leverage for individuals seeking to compromise election security.

Qualification of a system according to the Federal Election Commission's 2002 Voting Systems Standards provides some degree of assurance to a purchaser that a few security measures have been taken. Purchasers wishing to go beyond that degree of assurance might ask additional questions.[22]

[22]For example, Mulligan and Hall argue that current voting system standards (that is, the standards promulgated in 2002) are inadequate, and that systems fully certified as compliant with those standards exhibited critical problems due to gaps in the standards and the certification process, such as the lack of federal guidelines that speak to human factor issues in electronic voting. They further assert that the federal qualification system for DRE voting machines is inadequate and incomplete, and that significant problems evidently slipped through the cracks, resulting in polling place or tabulation failures in 2004. See Deirdre Mulligan and Joseph Lorenzo Hall, "Preliminary Analysis of E-Voting Prob-

4-10. **To what extent and in what ways has a realistic risk analysis been part of the acquisition process?** A risk analysis includes a threat model describing the various ways adversaries might exploit vulnerabilities in a system; a description of possible adversaries, their level of motivation and sophistication, and what resources they might bring to bear; an assessment of the likelihood of exploitation of various vulnerabilities and an estimate of the harm that might be done should exploitation occur; and a consideration of the possibility that an attack could be mounted without detection. For example, a postulated attack that involves the ability to improperly modify the code that will run on deployed voting stations presents security challenges that are very different from one that does not. Indeed, an attack involving insider access is much more serious, because of the possibility that the actions of a small number of individuals could have security ramifications in every deployment location (without such access a much larger degree of effort would be needed to achieve large-scale compromise).

In practice, a risk analysis must be undertaken by both vendors and election officials. A vendor must undertake a risk analysis in order to know what security properties a system must have. Development and design of the full system are not possible until the risk analysis has been performed. Though election officials—in their role as purchasers or lessors—are not responsible for system development or design, they too must undertake a risk analysis to determine if their own concerns about security are reflected in the vendor's analysis. For example, if the threats of concern to election officials are not reflected in the threat model used to analyze risk, the risk analysis is not likely to provide useful guidance to those officials. Also, election officials, with input from independent security specialists and the general public, may wish to formulate the threat models of most concern to them independently of the vendors' postulated threat models so as to avoid being captured by vendor biases.

---

lems Highlights Need for Heightened Standards and Testing," undated white paper contributed to the committee, available at http://www7.nationalacademies.org/cstb/project_evoting_mulligan.pdf.

The particular problem cited—the lack of guidelines relevant to human factors—was addressed explicitly in the proposed EAC revisions to the Federal Election Commission's 2002 Voting Systems Standards. The Technical Guidelines Development Committee of NIST was specifically chartered to address such shortcomings. But the pace at which the standards-setting process works remains an important issue. It is reasonable to anticipate that over the long run, the relevant guidelines will become more comprehensive. Nevertheless, at any given moment in time, there may well be important outstanding issues that have not been addressed in the standards.

4-11. **How adversarial has the security assessment process been?** Experience in the cybersecurity world has shown that adversarial techniques are generally the best for assessing security. That is, security should be assessed from the standpoint of an outsider trying to find exploitable flaws in it rather than an insider checking off a list of "good security measures." Indeed, a system may conform to the best of checklists and still have gaping security holes.

The best example of an adversarial assessment is the use of independent red teams, or "tiger teams," as described earlier.[23] Short of a red team attack, an independent adversarial examination of the "internals" of a system (physical construction in the case of hardware, actual code in the case of software) will provide some insight into its ability to resist attack, since it is likely to uncover flaws that an adversary might use. Moreover, in the absence of such an examination, it is not possible for any amount of testing to eliminate the possibility that the system will demonstrate some improper behavior under some set of circumstances. That is, testing may be a sufficient basis for concluding that a system does meet certain requirements (e.g., produces certain outputs when given certain inputs), but it cannot show that the system will not do something else in addition that would be undesirable.[24] Only by inspecting the internals does one have a chance of detecting the potential for inappropriate behavior when the system is put into use.

4-12. **How has the system's ability to protect ballot secrecy been assessed?** The same kinds of adversarial techniques used to assess security are also useful for assessing the ability of a system to maintain ballot secrecy. Box 4.5 illustrates some of the issues that might come up in such an assessment.

---

[23]An example of red team analysis is the "Trusted Agent" report on Diebold's AccuVote-TS Voting System, prepared by RABA Technologies LLC in January 2004 and available at www.raba.com/press/TA_Report_AccuVote.pdf. The red team analysis found that the Diebold system, which Maryland had procured for use in primaries and the general election, contained "considerable security risks that [could] cause moderate to severe disruption in an election."

[24]A simple example will illustrate the problem in principle. Using the logic described in Section 4.2.2 for maintenance traps, a system could be designed to change every 10th vote for Candidate A to Candidate B when a specific set of keys on the display is pressed in a specific sequence with a minimum time in between key presses. This particular example is contrived, as it would require quite a bit of skullduggery and the commission of a number of felony offenses on the part of a vendor, but the fact remains that no plausible testing process will ever uncover such a problem.

Box 4.5
Ballot Secrecy Considerations That an Independent Assessment Might Examine

Maintaining the secrecy of a voter's ballot is an important public policy consideration that is specified in state law. Known as "confidentiality" among computer scientists, the problem amounts to one of keeping the voter's ballot private under all circumstances. In particular, these circumstances include voter collusion (as might be the case for a voter trying to sell his or her vote); observations of voters and voter behavior in the polling place being correlated with voting station records; and corrupt insiders who might have access to voting station records. Put differently and more generally, computer scientists believe that a system properly designed to provide ballot secrecy must be able to defeat attempts to compromise the secrecy of an individual's ballot under all possible adverse circumstances.

In the absence of a specific system design, it is impossible to anticipate all possible threats to secrecy in anything but the most general terms. The following examples are intended to suggest a range of possible threats against which a system must be designed:

- The first person to vote on Election Day in her precinct may well be known to poll workers or others present at the precinct. A voting system that does not randomize the order in which ballots are reported will report this person's vote, and ballot counters will be able to recognize which ballot was cast first and thereby be able to easily deduce how she voted.
- A voter with a Vietnamese name requests a ballot in Vietnamese and is the only person with a Vietnamese name voting on Election Day in that precinct. If the system is designed to report votes as ballot images, it is easy to determine that one ballot is cast in Vietnamese and thus to associate with high probability this ballot with the Vietnamese-surnamed voter.
- If an electronic voting system is designed to produce a unique random 10-digit serial number on a cast vote record (e.g., so that a voter-verified paper audit trail of the ballot can be associated with the image),[1] a voter trying to prove how she voted (e.g., to sell her vote or because she has been forced to by a coercer) could identify her ballot by memorizing that serial number and then telling it to someone who has access to the cast vote records.
- If a DRE system is designed to record, next to each cast vote record, the sequence of selections and button presses performed by the voter to reach this cast vote record (e.g., to obtain information that might be useful in the design of future ballots for greater usability), a voter who wants to mark his or her ballot in an identifying way can use some distinctive sequence of button presses (forward, back, forward, forward, back, back, forward, back). This voter's ballot will be the only one that is recorded adjacent to that unusual sequence, and so this voter will be able to prove to anyone with access to this log how he or she has voted.

[1] A cast vote record is a stored record of the set of all of a voter's choices.

4.2.2.3 Deploying the Assessed System to Polling Stations

Qualification and certification testing of a voting system are only the first steps in the process of assuring end-to-end security. Even a voting system that has been qualified as secure, reliable, and easy to use is useless if it is not the system that voters use on Election Day. That is, the qualified and certified system must be deployed to polling stations for actual use on Election Day.

Acceptance testing is one element in providing such assurance. According to the Federal Election Commission's 2002 Voting Systems Standards, one purpose of acceptance tests is to ensure that the units delivered to local election officials conform to the system characteristics specified in the procurement documentation as well as those demonstrated in the qualification and certification tests. To help ensure that qualified voting systems are used consistently throughout a state, ITA labs can file digital signatures of qualified software with the software library of the National Institute of Standards and Technology (NIST).[25]

Acceptance testing is undertaken in the absence of a specific ballot configuration. Logic and accuracy (L&A) testing is the testing of voting systems configured with the ballot that will be used in the actual election. In principle, L&A testing serves two main functions—to account for any changes to a unit's configuration between the point of acceptance and Election Day, and to ensure that the unit performs properly with the actual ballot to be used. Thus, L&A testing can be usefully applied to every unit that voters will use in the election, although the expense of testing generally allows only a fraction of those units to be tested. When units are known to be identically configured, only one of them needs to be thoroughly tested and the rest tested simply to ensure that no failure has occurred.

These two types of testing motivate several additional questions:

4-13. **How is the security of voting stations maintained to ensure that no difficult-to-detect tampering can occur between receipt from the vendor and use in the election?** In theory, this is a straightforward matter—put the voting stations in a locked building with no remote access to

[25]A digital signature is a unique, algorithmically generated fingerprint of any digital object (such as a software module). By comparing signatures, one can easily determine if two objects are identical. NIST maintains a library of certified code to which ITAs can submit qualified election software versions, with a digital signature that enables states and local election officials to check whether individual machines utilize exactly the same software. But even the smallest change in software will change the signature (for example, the code for "3 + 2" will have a very different signature from the code for "2 + 3"). Practical difficulties of performing such a check are addressed in Footnote 28.

them and ensure that no one has access until they are removed for use on Election Day. But there are several factors that complicate this simple picture. For example:

- Vendors may need access to load ballots to individual voting stations, a task that must be performed before Election Day.[26] However, the steps that must be taken to load ballots may, or may not, resemble those needed to change software. How will those supervising the loading of ballots be certain that no other changes are being made to the voting stations?
- Third parties may masquerade as election officials or vendors and demand access to the voting stations in storage. Or moles (individuals with ostensibly authorized access but who in fact have been compromised to work in a partisan manner) may be present in the offices of election officials. What procedures are in place to guard against changes introduced by these insiders (for example, a rule that requires that access to systems in storage is never associated with only one or two persons)?[27] How rigorous are the procedures for ensuring that only properly authorized parties have access to the storage facilities?
- Early voting, an increasingly common practice that entails taking voting stations out of storage before Election Day, further complicates the achievement of security and chain-of-custody goals.

4-14. **What steps have been taken (either technically or procedurally) to limit the damage an attacker might be able to inflict?** As a practical matter, the compromise of one voting unit in one precinct is obviously less harmful than the compromise of all of the units in the entire jurisdiction. One approach to limit possible damage is to ensure that modifications or updates cannot be made en masse, that is, through one action updating all units. Thus, a large-scale compromise would entail significantly more effort for the attacker than a small-scale one. Of course, this approach makes it much more inconvenient and costly to deploy updates when they are necessary.

---

[26]In principle, election staff could do so as well. But given the prominent role that vendors have often been given in providing supporting services (Section 6.7), it is entirely possible that vendors may have this responsibility.

[27]The insufficiency of a two-person rule has been noted in the finance industry, in which audit procedures typically call for involving three or more individuals. The reason is that if one party in a two-person conspiracy breaks the secrecy pact, his or her identity is known with certainty to the other party. However, if the conspiracy involves three or more individuals, the identity of the party breaking the secrecy pact cannot be inferred with certainty by any of the others. In an election context, such a procedure might involve representatives from two parties jointly picking a third.

4-15. **How can election officials be sure that the voting systems in use on Election Day are in fact running the software that was qualified/certified?** For example, a vendor may uncover a potentially problematic issue in software that has been previously certified and address the issue in a program patch. Strictly speaking, any change to a program requires recertification, and some state laws require recertification after every software change, no matter how small. But because full recertification generally takes a long time (in principle, as long as the initial certification), there are strong incentives for the vendor to argue that the change can be administratively approved.

The question then arises whether the change involved is small enough to be addressed administratively. In the absence of specific criteria, vendors are in the best position to know about the scope and significance of any change. On the other hand, from the point of view of an outsider without such privileged knowledge, the nature of programming is such that it is essentially impossible to assure that changes made in one part of the program will have no effects on other parts of the program. Without inspecting the code involved (and the other parts of the program with which it interacts), there is no way to determine if a change is significant or not. Some evidence may be forthcoming if the original program is designed in a modular fashion with well-documented interfaces, the behavior of existing modules is understood, and the changes are confined to one or a few modules. But the mere assertion of a claim does not suffice for most outsiders.

If an administrative certification is not possible, election officials have the operational choice in practice between running certified code that may have problems or running uncertified code that has been fixed. Thus, some election officials may still try to think of ways to avoid this certification step, particularly if they know that a smooth election process depends on a last-minute fix.

A related issue is that despite precautions that have been taken, software may have been compromised through the introduction of an unauthorized patch. Beyond vendor assurances, what technical means are available to demonstrate that such compromise has not taken place? For example, a digital signature of the software running on any given station can be taken for comparison with a known version, though this is difficult in practice today.[28]

[28]The difficulty arises because the software for most electronic voting systems resides in a programmable read-only memory (ROM) module soldered to the system's motherboard, and obtaining access to the module's contents in practice is today a cumbersome and labor-intensive process that entails physical removal of the module. Moreover, short of a readout of the ROM's contents and the computation of the digital signature, there is no way to independently ascertain which version of software is in fact running on a given station.

A second related issue is that the source code for software running on an electronic voting system may not be fully available.[29] Some vendors of electronic voting systems may build their systems using the foundation of a (proprietary) commercially available operating system. Device drivers (programs that manage the devices attached to a computer) may also be available in object code but not in source code. (As a rule, systems that are based on the use of such commercial off-the-shelf components are generally less expensive and faster to develop than systems that are custom-designed and implemented from the ground up.) In this case, there is a strong sense in which the certification or qualification of voting system software is necessarily conditional (perhaps implicitly), because it presumes that the operating system or device drivers, or interactions between the voting application and the operating system or device drivers, do nothing strange or unexpected or malicious. Furthermore, vendors or jurisdictions managing relatively small contracts will not generally have enough leverage with the provider of operating systems or device drivers to obtain source codes for inspection.

4.2.2.4 Using the Deployed Units on Election Day

In general, the issues on Election Day are more likely to be associated with reliability than with security. That is, if rogue voters are able to compromise the security of the voting systems they use, it will almost certainly be through the Election Day exploitation of a pre-existing security vulnerability. Such situations are covered under Sections 4.2.2.2 and 4.2.2.3.

The one exception is what might be called a denial-of-service attack against voting systems in use. For example, Party A might try to deny service in an area with large numbers of people from Party B, thus reducing the turnout and vote count for Party B. Lack of availability of even a few voting stations for even a short amount of time during peak hours can result in very long lines for voting, leading to voter discouragement and an effectively lower turnout.[30]

---

[29]Source code refers to the software in the form in which it was originally written—usually in a high-level programming language that is understandable to humans. Object code refers to the corresponding ones and zeroes that actually run on a computer. Programs known as compilers are required to translate source code into object code.

[30]An example of such a threat might involve a set of voting stations connected via a wireless LAN to a central monitoring station in the precinct. A system might be vulnerable to electronic jamming in the precinct that would prevent the voting stations from communicating with the central monitoring station and might thus be prevented from accepting input at all. (Perhaps for this reason, no present electronic voting system is based on this architecture.)

From the standpoint of assuring election integrity, Election Day is also an opportunity to collect data that can be used later to audit the election and to document anomalies that might point to systemic problems that need remediation in the future.

4-16. **What information must be collected on Election Day (and in what formats) to ensure that subsequent audits, recounts, or forensic analysis can take place if they are necessary?** As noted in Chapter 1, elections may be subject to post-Election Day challenge. To resolve such challenges after the fact (of the election), information about what happened on Election Day must be available. Challenges to the vote as recorded and communicated by the voting station and the tabulation equipment might arise from a sufficient number of individual voters wanting evidence of how their voting intent was interpreted, or from systemic difficulties due to bad system design or fraud. Should an audit become necessary (because irregularities are charged or because a state's best practices mandate random audits), auditors need data and records to examine. It is therefore essential that a locality collect such data before and during the election so that appropriate records are available. An example of data that might support an audit is exit poll data, which might be collected by the state rather than a media organization, for later comparison to actual totals.

This point is the primary motivator of various demands for paper trails in electronic voting systems—the concern expressed by many advocates of paper trails is that a DRE system without such a capability is unaccountable, and that such systems give election officials who are challenged the stark choice between accepting the numbers proffered by the system and redoing the election.

Box 4.6 provides some examples of relevant data that are arguably relevant for forensic analysis.

4-17. **How are anomalous incidents with voting systems reported and documented?** Given that in-use operations are the ultimate test of voting systems, it is important to capture as much information as possible about how voting systems perform in actual use. What incident-reporting structure will guarantee that problems are reported promptly to vendors, to states, to other local election jurisdictions within the state using the same systems, and to standards-setting organizations? How can knowledge of these anomalies be used to improve voting system performance?

For example, Florida certified an electronic voting system despite the fact that the voting machines took a long time to boot up and machines had to be opened in sequence. It took between 90 minutes and 4 hours to open a precinct. Therefore, the machines could not be turned on the same day that an election took place. The certification standards had not ad-

Box 4.6
Election Administration Information Required for a Complete Audit

1. Data to collect before the election:
   a. Local voter registration numbers and lists. [P,S]
   b. Inventories of equipment and ballots upon acceptance (e.g., date of purchase, source, maintenance records, vendors, serial numbers, retain code versions in offsite escrow). [S]
   c. Seal numbers for ballots and machines and storage locations for voting equipment. [S]
   d. A record of personnel with access to equipment, including detail such as when and where. [S]
   e. Changes made to the equipment (e.g., oiling, charging, battery changes, memory upgrades, putting in a module, checking odometers, code drop). [S,P]
   f. A list of the times and modes by which voting equipment is transported (including license plate number and driver for chain-of-custody purposes). [S]
   g. Inventory of equipment and materials before and after transportation. [S]
   h. Inventory of equipment and materials before voting begins. [S]
   i. Pre-election equipment testing data, including the number of systems tested and problems observed during testing. [S,P]
   j. Number of training sessions held for poll workers, and a roster of poll workers attending each session. [P]
   k. Copies of sample ballots and voter information materials. [P]

   When electronic voting systems are involved:
   - *Date of most recent software update.*
   - *Type of certification for software update.*
   - *Comparisons of digital signatures of software running on individual voting stations with digital signatures in NIST's National Software Reference Reference Library.*
   - *Results of logic and accuracy testing.*
   - *Contingencies for which the poll workers were trained.*
   - *Physical security maintained on voting station.*

These data help assure that ballots, equipment, and polling places are usable and also makes it possible to deal with problems and questions that may arise later.

2. Data to collect during the election:
   l. Number of poll workers at each poll, including the times at which poll workers arrive and leave. [S]
   m. Signatures (not check marks) of those present. [S]
   n. Signatures for inventory received election night, both in precincts and when inventory is returned to the central office. [S]
   o. Tally at precinct and time it was conducted. [S,P]

p. The number of poll and early voting sites and any rents required to use these locations. The number of workers in each poll or early voting site, their rate of pay, and their required number of hours of work. [P]

q. If "parallel testing" is conducted on Election Day, the number of voting machines tested, the way in which they were selected for testing, and the results of those tests. [S,P]

r. Exact time when each poll site opened. [P] (Maximum waiting times at each poll site.)

s. The number of poll sites that experienced significant problems, an explanation of the problems experienced, and a description of how these issues were resolved. [P,S]

The number of individuals turned away from the polls and the reasons they were turned away.

When electronic voting systems are involved:

- *Frequency of restarts and reboots required for voting stations.*
- *Descriptions of anomalous behavior during use.*

These data will ensure that processes during the election are monitored. They also give the best possible means to later establish what voters' intentions were, and that they were allowed to vote correctly.

3. Data to collect after the election:

t. Inventory of equipment and materials after polls close. [S]

u. The total number of ballots cast (report absentee and poll site totals separately, if possible). [P,S]

v. The number of votes cast for all candidates for each federal and local office (reporting absentee and poll site totals separately, if possible). [P]

w. The number of registered voters. [P,S]

x. The number of people who voted as indicated on check-in/check-out lists. [P,S]

y. The numbers of absentee ballots applied for, tabulated, and challenged. [P,S] The reasons for any successful challenges to such ballots.

z. The number of absentee ballots received, recorded by date received. [P]

aa. The number of absentee ballots returned from citizens residing outside the country, and the number of these that are challenged. [P,S]

bb. The number of tabulated provisional ballots provided to voters that were challenged. [P,S]

cc. The number of early voters. [P]

dd. Transportation records of equipment (consistent with above criteria). [S]

ee. Storage records of materials. [S]

These data establish the ability to know that votes were handled and reported correctly. Furthermore, they give people the ability to know how to improve processes for future elections.

4. Demographic and administrative data:

continued

Box 4.6 Continued

ff. The annual expenditures for election administration, including personnel and capital expenditures. [P]

gg. The number of physical voting sites and the number of precincts (if not the same because of consolidation) used in the election. [P]

hh. The number of days in which early voting is allowed, and the number of early voting sites operated. [P]

ii. Census demographics of voting precincts, if available. [P]

jj. Salary, by job category, of poll workers for the election, details of their job qualifications and hiring process, and years of experience. [P,S]

kk. Type of election administration system (e.g., elected or appointed board, elected or appointed registrar). [P,S]

NOTE: "P" indicates data critical for undertaking performance audits; "S" indicates information critical for security audits. Where the information can be used to audit both performance and security both letters are used, in order of priority.

SOURCE: Nonitalicized material is taken from the Caltech/MIT Voting Technology Project, *Insuring the Integrity of the Electoral Process: Recommendations for Consistent and Complete Reporting of Election Data*, October 2004, available at www.vote.caltech.edu/media/documents/auditing_elections_final.pdf. Italicized material originates with the committee. The Caltech/MIT Voting Technology Project proposed that the above set of (nonitalicized) data at the precinct level be collected, retained, and distributed for every federal election in the United States in order to support postelection audits should they become necessary.

dressed the time required to open the machines or the time required to open average precincts or large precincts—elements that proved important to using the machines. After the problem was identified, the state certified a new version of the software that permitted somewhat faster opening of the polls. A few minutes after one machine began booting up, the clerk could begin opening the next machine. However, the standards were not changed to make speed in opening the polls an element of certification.

4-18. **What is the role of parallel testing?** Parallel testing, which is intended to uncover malicious attack on a system, involves testing a number of randomly selected voting stations under conditions that simulate actual Election Day usage as closely as possible, except that the actual ballots seen by "test voters" and the voting behavior of the "test voters" are known to the testers and can be compared to the results that these voting stations tabulate and report; this exception is not available (because of voter secrecy considerations) if the parallel testing is done on Election Day. Note also that Election Day conditions must be simulated using real names on the ballots (not George Washington and Abe Lin-

coln), patterns of voter usage at the voting station that approximate Election Day usage (e.g., more voters after work hours, fewer voters in mid-afternoon, or whatever the pattern is for the precinct in question), and setting of all system clocks to the date of Election Day. Parallel testing is a check against the possibility that a system could recognize when it is being used on Election Day and report undoctored results when it is being tested at any other time. An important issue in parallel testing is how many stations must undergo parallel testing in order to provide reasonable assurance that inappropriate behavior has not occurred.

4-19. **What physical security provisions will be put into place at polling places after the voting stations have been delivered but before the polls open?** Physical security is the primary barrier to unauthorized changes in the configuration of individual units. In the period after delivery of voting stations to polling places but prior to the opening of the polls, physical security must again be maintained—the procedures required are generally the same as when the voting stations are in storage but must now be carried out in different locations. (Note that an important characteristic of polling places staffed by poll workers is that the workers provide some degree of control over physical access to voting stations, as compared, for example, with a home computer used by a voter to cast or mark a ballot, either by mail or—in the future—using a personal computer. Internet access for such a voting station would introduce additional possibilities for making unauthorized changes.)

4-20. **What physical security provisions will be put into place immediately before the polls open and immediately after the polls close?** Poll workers are generally responsible for initializing voting stations so that the internal counts in each station are set to zero and for delivering station totals to the central tabulation authority. Unless special precautions are taken against the possibility of a compromised or partisan poll worker, these are the points on Election Day at which tampering is most likely to occur. For example, special security precautions might include requiring individuals from more than one party to be present for station initialization, each of whom is familiar with what is and is not necessary to initialize the station. If this practice were not followed, someone could be selected at random to perform initialization.

4-21. **What physical security provisions will be put into place at polling places while the polls are open?** While the polls are in use, a different set of physical security issues arises. Voters will be using these units for periods as long as many minutes, and voter secrecy considerations preclude any kind of monitoring that might be intrusive from the voter's perspective. Poll workers may also be busy with checking voter registration, so they may not have time to perform such monitoring in any case.

4.2.2.5 Aggregating/Tabulating Voting Results

Election outcomes are determined by aggregating the votes cast at all the polling places. Individual votes can be directly counted by a central authority, or aggregated at the level of the individual voting station. Either case entails communication between the voting machines at each location and some central authority responsible for tabulation, and individual unit counts are usually transmitted at the end of the day.

4-22. **How are the results from polling stations communicated to the central tabulation authority?** Because the results from every voting station must be included in the final tally of votes, there must be some mechanism for communicating this information to the tabulation authorities. (Results may be conveyed as station subtotals for various contests or as individual untallied records of the individual votes cast—the "cast vote records.") There are only three ways for this task to be accomplished: manually at each station (e.g., by someone reading vote totals at each station and transferring the numbers to a notebook or ledger, or talking into a telephone); by the physical removal of some computer-readable media from the station that contains vote totals; and by direct transmission over some wired or wireless medium such as a modem and telephone lines and computer network (as was the case with the Department of Defense SERVE prototype; see Box 3.1). These methods may also be used in combination. For instance, if security were an issue, a wired or wireless medium might be used to provide preliminary data, while the official data might be transported via secure couriers carrying flash memory cards.)

Each of these methods entails different risks. Reading vote totals at each station and transferring the numbers manually raises issues of human error in recording vote totals as well. For example, a person reading numbers over the phone might be misunderstood by the receiver of those numbers, or the handwriting in a written record could be misread, or the numbers could be wrongly transcribed. Manual handling of the numbers and the use of computer-readable media for recording the vote totals both raise issues of physical custody of the ledger or media in transport to the tabulation authority. For example, if precautions are not taken, an adversary could substitute a CD-ROM prewritten with the appropriate vote totals for the CD-ROM taken from a specific voting station. Direct transmission of vote totals over a wired or wireless network renders the transmission vulnerable to spoofing attacks, in which the receiving computer is tricked into accepting numbers from an unauthorized source; or the transmission could be intercepted, modified, and played back; or a denial-of-service attack could take place in which the input channels on the receiving computers are blocked.

Procedures and/or technologies are available to deal with all of these problems, but they all require special attention to think of these problems and then to implement the available solutions. (For example, one element of guarding against the substitution of an unauthorized CD-ROM for an authorized one containing voting information might call for multiple poll workers of different parties to accompany the CD-ROM to the counting facility.)

4-23. **How does the central tabulation authority aggregate vote totals?** In general, computers will be responsible for tabulating the results from individual voting stations. But all of the concerns about software security expressed earlier in the context of individual voting stations apply as well to software at the central authority, with the possible exception that physical security is likely to be easier to maintain in a single place than in many precincts.

4-24. **What physical security provisions will be put into place at the central tabulation authority?** For example, because of the sensitivity of the tabulation operation (aggregating records from all polling stations), one might argue that physical access to the facility should be carefully controlled (e.g., all persons entering or leaving the tabulating center might be required to provide legal identification and sign in and out on a public log as an elections employee, a temporary employee, a contractor, or a visitor. Operations at the facility might also be recorded on videotape.

4-25. **What roles can postelection auditing and investigation routinely play to increase the likelihood that fraud or other problems will be detected?** Some legal regimes governing elections require that a postelection audit be performed automatically if the margin of victory for any candidate or proposition is less than a certain percentage. In other regimes, losing candidates can (and often do) request a recount if the margin of victory is less than a certain percentage. (In California, 1 percent of all precincts are audited routinely after each election, with the intent of using the results to uncover problems and make improvements in future elections rather than trying to find fraud.)

The assumption implicit in legal regimes based on the magnitude of a margin of victory is that the effect of anomalies is small—that only a few of the votes cast were not properly counted. According to this logic, a large margin of victory renders the presence of anomalies more or less irrelevant in the practical sense of affecting the outcome of the election; only when the margin of victory is small could anomalies matter.

In a precomputer era, this assumption was easily defended. Large-scale anomalies would require a large-scale effort and a large number of human beings, thus increasing the likelihood that the perpetration of anomalies would be detected by the authorities. But, as noted earlier in Section 4.2.2 on the possibility of automated fraud, the concern of com-

puter experts is that a small number of corrupt or compromised individuals might be able to conduct their dirty work so that they would have a very large effect.[31] To guard against such a situation, some security specialists advocate routine auditing, security review, or other investigation in the wake of an election; such auditing would have a chance of finding attempts at fraud that various testing and/or code inspection procedures had not discovered.

4.2.3 Usability and Human Factors Engineering[32]

4.2.3.1 Perspectives on Voting System Usability

All voting systems face the usability problems of accurately capturing the voter's intent in casting a ballot and of being easy for voters to use, both of which are exacerbated by the vagaries of human behavior. Indeed, the importance of usability is highlighted by the role of the infamous butterfly ballot in the 2000 presidential election in Florida, which allegedly confused many voters into casting a ballot that was contrary to their intent. Electronic voting promises many advantages from a usability standpoint, but there is no single best way to capture voter intent. Consequently, different vendors and different election officials can legitimately and ethically make different decisions about how best to present information to the voter and how best to capture the voter's vote.

One quantitative measure of a system's usability is the error rate of

[31]A particularly worrisome scenario is that corrupt partisans might modify vote totals so that the margin of their candidate exceeds that required by law for recounts, precluding a recount or any other subsequent closer examination. Alternatively, corrupt partisans might modify vote totals so that the margin requires the loser to pay the full amount of the recount, effectively making a recount unaffordable by the challenger. In other words, by adjusting the vote totals carefully, corrupt partisans could create an apparent margin of victory large enough to make unlikely or impossible a recount or an audit that might reveal the fraud.

[32]The discussion in this section mostly concerns electronic systems that are used to capture voter ballots directly. Today, these systems are for the most part direct recording electronic systems. Optical scan systems are another important type of electronic voting system, but in optical scan systems the voter marks up a paper ballot that is then scanned electronically. Thus, the mechanism for capturing voter intent is paper-based rather than electronic, and the considerations of this section are mostly not relevant to optical scan systems. This subsection draws in several places from Harry Hochheiser, Ben Bederson, Jeff Johnson, Clare-Marie Karat, and Jonathan Lazar, *The Need for Usability of Electronic Voting Systems: Questions for Voters and Policy Makers*, Association for Computing Machinery (ACM) Special Interest Group on Computer-Human Interaction (SIGCHI), U.S. Public Policy Committee, white paper submitted to the committee. Available at http://www7.nationalacademies.org/cstb/project_evoting_acm-sigchi.pdf.

that system in capturing votes—an error would be the recording of a vote that was contrary to the voter's intent in casting the vote, and the error rate would be the fraction of all votes recorded that were in error. If the error rate is x percent, then an election that is decided by a margin of less than x percent cannot necessarily be said to reflect the intent of the voters. While careful attention to usability issues can force x to be lower than it would otherwise be, x cannot be driven to zero. A design issue is then what the appropriate value of x is for any given system.[33]

Lowering the error rate of a system in use is the domain of what has come to be called human factors engineering. This is an interdisciplinary field that includes cognitive psychology, the ergonomics of sensing and making manual responses, and systems engineering. The field is largely experimental, much as is the field of medicine, making heavy use of statistics to draw inferences from human subjects in spite of their variability. The end goals of human factors engineering are the design of a technology to make it safe and effective for human use and to develop procedures for machine operation and training for the maintenance and management of the technology.

In recent years human interaction with computers has been a major component of human factors engineering. This includes not only standalone computers but also computers embedded in a variety of systems: aircraft piloting and air traffic control, military and space systems, manufacturing plants, hospitals, business and banking systems, and, more recently, automobiles, homes, and special-purpose computing appliances such as personal organizers and digital music players.

For much of the past, usability issues in voting systems were limited to a consideration of physical accessibility on the part of the voter and translation into non-English languages for non-English-speaking voters. But as the 2000 election demonstrated so clearly, there is much more to usability than access. Indeed, in a voting context, usability includes many things: human behavioral constraints (perceptual, cognitive, and motor capabilities); background (language, education, culture, past experiences); complexity and extent of the task (arrival, departure, waiting in line, ask-

[33]For a sense of the order of magnitude of x in practice, Ansolabehere and Stewart estimate that the residual vote due to technology factors is on the order of 1 percent; see Stephen Ansolabehere and Charles Stewart III, "Residual Votes Attributable to Technology," *Journal of Politics* 67(2), 2005. Recount data also provide indicators of error rates, and these are in the 0.5 to 1 percent range; see, for example, Stephen Ansolabehere and Andrew Reeves, "Recounts and the Accuracy of Vote Tabulations: Evidence from New Hampshire Elections 1946-2002," CalTech/MIT Voting Technology Project Working Paper, January 2004. Available at http://www.vote.caltech.edu/media/documents/wps/vtp_wp11.pdf.

ing for help, etc.); situation and environmental contexts, such as the physical situation (adequacy of lighting, electricity, heating, etc.) and the social situation (crowds and time limits); sociological issues (privacy, confidence in technology, and equity issues); psychological factors (workload, attention, situation awareness, and distractions that constrain people's actions); political factors (e.g., proper randomization of candidates, allowing for straight ticket voting); and different perceptions on the part of designers and users of what a system should do.

Design for human usability, like any kind of design, is an art informed by experimental findings that have been reported in a growing scientific literature. This includes handbooks, guidelines, and checklists developed for particular applications. Guidelines applicable to voting systems might include the following:

1. *Task analysis*. A first order of business is to understand what the basic voting task is, not what specific objects or events the voter must see or hear or what particular responses must be made but rather what information must be communicated to the voter (from the machine, the physical environment, and the poll workers), what information must be communicated from the voter (to the machine, the physical environment, and the poll workers), and what decisions must be made by the voter, the poll workers, and the machine at particular stages of the task. Appreciating the task at this abstract level is essential to considering the design alternatives and pitfalls. There are many formal methods of task analysis involving space, time, probability, causal contingency, and so on.

2. *Sensing constraints*. What people perceive and discriminate depends on physical variables, expectations, and attention. In vision, these variables include size, brightness, contrast, color, and time duration. Hearing and touch are similarly dependent on a corresponding array of physical variables, though these factors generally play a lesser role for most voters using a voting machine. The minimum perceptible and differential (discrimination) thresholds and trade-offs among these variables are well established in the human factors literature.

3. *Cognitive constraints*. What people understand and remember from what they perceive depends on more subtle aspects of natural language and symbol familiarity, cultural norms, education level, one's mental model of how something works, situation awareness, memory, mental workload, basic mental capacity, and so on. What a voter decides depends on clearly understanding the decision alternatives.

4. *Response constraints*. Appropriate voter response depends not only on what candidate choice the voter intends but also on knowledge of how to respond so as to communicate that choice to the machine. This may be easy or difficult, depending on physical variables such as location of re-

sponse devices (buttons, levers, sensitive areas of a touch screen, force levels and accuracy thresholds of response motion, etc.). It also depends on evident correspondence (in location, direction of response motion, sequential order, label wording, etc.) of the appropriate response to the stimulus (e.g., name of the candidate). This is what human factors professionals call stimulus-response (or display-control) compatibility. It is the criterion that the infamous butterfly ballot flaunted.

5. *Error types, causation, and remediation*. Human errors can be classified in different ways, and such classification is a step toward understanding their causes and preventions. Errors can be omissions (correct action not taken) or commissions (actions taken that ought not to have been taken). Errors can be slips (intended action not taken) or mistakes (intended action taken but turning out to be inappropriate). Errors can occur at any of the stages of sensing, remembering, deciding, or responding.

Human errors often result when people do not receive sufficient feedback in a timely and understandable way. In daily living, people constantly get such feedback from their physical and social surroundings. Other common error causes are inappropriate mental models of how something works, forgetting, distraction, incorrect expectations (e.g., performing a task in a habituated way when present circumstances call for a deviation from the norm), lack of sufficient stimulus energy, or mental or bodily incapacity.

The best way to prevent error is to design the machine or process to be easy (simple, obvious) to use, and this includes good feedback, even in redundant ways. Education and training are next most important, but best designs also minimize necessary training. Computer-based decision aids and in situ guidance, alarms, and prevention of exposure to the opportunity to err (the computer will not recognize certain commands under some circumstances) are other techniques used. Posted warnings have proven to be the least effective means of preventing errors. A well-designed system with adequate feedback will allow the user to commit an error, observe the error, decide what to do about it, and gracefully recover from it.

6. *Training*. What is obvious to the designer of any machine or process is often not so obvious to the user. Any experience that differs from what one is accustomed to is likely to trigger some confusion. Therefore, at least a modicum of training will be essential for electronic voting. Some training can be accomplished by a well-designed brochure made available either prior to or at the site of voting. It can be augmented by poll workers explaining features of the machine or process that may be confusing. A more sophisticated approach used in some computer-based systems is to embed the training—that is, have the voter go though a few steps of observation and response to displayed dummy candidates to

ensure that the voter understands the system. Training is also important for the poll worker, who are often senior citizens less familiar with and more anxious about using computers than the majority of the voter population.

7. *Interaction with automation*. Human interaction with computer-based machines that may be said to embody at least rudimentary intelligence poses special problems. These may occur for poll workers or technicians employed to set up the machines, make sure they are working properly, understand indications of machine failure (and curtail their use if necessary), and transfer voting data from them to other repositories. It is common that the user attributes more intelligence to a computer than it has. It is also common that a mode error is committed—namely, the user assumes that the machine is set in one mode and takes actions appropriate to that mode, when in fact it has been set to another mode and the action produces an undesirable result.

8. *Experimentation and simulation*. Experimentation and simulation are essential to system design, setup, voter and poll worker training, and evaluation of voter confidence and system effectiveness. Dealing with human subjects is a special art. Because of the special challenges of dealing with the great diversity of voters and poll workers with respect to education, technological sophistication, and physical and mental limitations, great importance must be attached to well-designed simulation trials, with voter subjects drawn from the representative population. Experimental designs must include a sufficient sample size and proper allocation of subjects to experimental runs to minimize bias in resulting data. Only then can designers of machines and training regimens feel confident, and only then can conclusions about system effectiveness and voter confidence be made.

Voting systems pose a particularly difficult usability challenge. They must be highly usable by the broad public.[34] As Hochheiser et al. point out, a citizen in the voting booth facing an electronic voting system may not feel comfortable with information technology, may not be literate (in terms of everyday reading and writing and/or with respect to using a computer), may not be an English speaker, and may have physical, perceptual or cognitive disabilities that interfere with understanding the bal-

[34]Voter registration database systems are another example of an election-related information technology, and as such, user interface issues are important to their users as well. But the population of intended users for these systems—those involved with election administration—is very different from the general adult population at large (that is, those who are part of the population of potential voters). As one example, election officials are likely to interact with a voter registration database system frequently, whereas voters are likely to interact with a voting system only rarely.

Box 4.7
Usability Issues That an Independent Assessment Might Examine

- Are voting station controls clearly labeled?
- Are fonts readable?
- Is consistent language used throughout the interface?
- Can users easily change votes once selected?
- Are write-in votes easy to cast, with clearly labeled choices?
- Are controls laid out so as to minimize the likelihood of accidental completion of a ballot?
- Have user interfaces been designed for use by and tested by a wide range of users of varying levels of expertise, education, and literacy?
- Have user interfaces been designed for use by and tested by voters with various disabilities, including (but not limited to) poor vision/blindness, motor impairments, and cognitive difficulties?
- Has the testing been conducted in environments that approximate the stresses and distractions of real polling places?
- Does the system provide adequate feedback that the vote intended was indeed captured?

SOURCE: Harry Hochheiser, Ben Bederson, Jeff Johnson, Clare-Marie Karat, and Jonathan Lazar, *The Need for Usability of Electronic Voting Systems: Questions for Voters and Policy Makers*, Association for Computing Machinery (ACM) Special Interest Group on Computer-Human Interaction (SIGCHI), U.S. Public Policy Committee, white paper submitted to the committee. Available at /cstb/project_evoting_acm-sigchi.pdf" http://www7.nationalacademies.org/cstb/project_evoting_acm-sigchi.pdf.

lot, interacting with the system, and casting a vote. This citizen is probably alone in the booth and may not be able to, or may be socially inhibited from, asking for help. Finally, most citizens vote no more than once or twice a year and thus have little opportunity to develop experience or familiarity with the system. Box 4.7 addresses some of the issues that might be examined in a usability assessment.

4.2.3.2 Design for Effective Use

The first stage in the life cycle of a voting system is requirements development and design. The top-level requirement is relatively simple: the system must capture the voter's vote as he or she intended it. However, designing a system to do this under a wide variety of circumstances is a nontrivial task. Questions related to design include the following:

4-26. **How does a voter receive feedback after he or she has taken an action to cast a vote?** After the voter has pressed a button or touched a screen, a natural question for the voter to ask is, "Did the machine accept my input?" or "How do I know my vote was entered?" While punch card, optical scan, and lever voting systems involve physical artifacts that provide immediate feedback to the voter about the choice or choices that have been made, the workings of electronic voting systems are more opaque from the voter's standpoint. Indeed, in some electronic voting systems, feedback mechanisms must be explicitly designed in. (In this context, this question is a user interface question rather than a security question. That is, it is assumed that the software is not trying to trick the voter into believing something that is not true.)

Note also that the presence of some feedback does not solve all user interface problems. Useful feedback both informs the user that an action was recorded and indicates which action was accomplished. For example, a click sound and the appearance of an X in a selection box indicates that a selection was made but not necessarily which selection was made. If the box is not clearly located next to the appropriate option, or the option is not highlighted when selected, a user may not know which specific option was selected.

In the case of the Florida butterfly ballot of 2000 (a punch card ballot), voters received feedback about having punched a hole in the card. But the ballot nevertheless confused voters about which selections they had actually made. One possibility is that voters did not punch the card fully; a second possibility is that poorly maintained machines made it impossible to punch the card fully. In both cases, the result would have been some ballots with "hanging" and "dimpled" chads—and doubt about the validity of those votes. At the same time, the voter would not know that the ballot cast might not be interpreted as a valid vote. A third possibility is related to ballot design—some number of votes appear to have been inadvertently cast for the wrong candidate because of misalignment of the punch hole locations and the candidate names—and the voter may have cast a vote for someone other than his or her actual choice without knowledge of that error.

4-27. **How is an electronic voting system engineered to avoid error or confusion?** Both the display and control interfaces of the system and the logic enforced by the system are at issue. For example, a large ballot may need to be presented to the voter on multiple display screens. What feedback does the system provide to the voter about where he or she is in the ballot? What provisions are made to enable the voter to back up, go forward, and jump around the ballot? To retrace his or her steps? To review the entire ballot before submitting it? As for logic, systems can be designed to block actions that would invalidate a vote or to warn the

voter of possible errors in the ballot before the ballot is cast, thus providing an opportunity to correct his or her ballot. For example, a direct recording electronic (DRE) system can prevent a voter from overvoting by forcing the selection of an "excess" choice to result in the deselection of a previously selected choice, or by not allowing new selections beyond a certain number and generating a message that informs the voter of a mistake. In the case of undervoting, a DRE system can warn a voter if a particular contest has been left blank but without forcing him or her to cast a vote in that contest.[35] (Both punch card and optical-scan voting systems can warn voters of overvotes if ballots are counted in real time by a precinct-based system.)

4-28. **What accommodations have been made to address the special concerns and needs of people with disabilities?** Citizens with disabilities have a right to a voting experience that is fair and acceptably straightforward—a requirement that is codified in the Help America Vote Act of 2002. Note that these issues are not simply problems of technology. In some instances, assistance from poll workers may be necessary.

4-29. **What accommodations have been made to address the needs of non-English speakers, voters with low literacy skills, and citizens from various cultural, ethnic, and racial groups**? All citizens have a right to vote regardless of their background, language group, or cultural situation. Electronic voting systems offer the possibility that a ballot can be easily switched to different languages or rendered audible for nonreaders.

4-30. **How and to what extent have concerns about the needs of these parties been integrated into the design of the system from the start?** A substantial body of experience indicates that attention to such concerns is much more effective at the start of the design process than at the end, at which point other decisions have been made that eliminate options that might otherwise have been desirable. (For example, a "screen reader" that tries to render a written ballot into words is often not as successful as a ballot that is designed from the beginning to include auditory interaction.)

4-31. **What are the ballot definition capabilities offered to jurisdictions?** Ballot definition is the process through which the ballot pre-

[35]Error checking can also create voter dissatisfaction. For example, some voters have become accustomed to nonelectronic systems that do not perform error checking. If they violate the ballot logic (e.g., an overvote), their votes do not count, but they have no way of knowing this fact if the votes are tabulated remotely. When faced with an electronic voting system that does perform error checking, the voter may react negatively because it is preventing him or her from voting in the accustomed manner.

sented to the voter is laid out. It involves aspects such as font size, graphics, placement and formatting of items, translation into other languages, and so on. Ballot definition issues were responsible for the problems with Florida's butterfly ballots in the 2000 presidential election. In practice, a voter's experience is determined by some mixture of the system's devices for entering input and the appearance of the ballot to the voter. Voting systems must be usable with a wide variety of ballots. That is, a vendor may wish to sell systems to multiple jurisdictions, each of which has different ballot requirements. Even within the same jurisdiction, a number of different ballots may be involved. Ballot design directly affects the ability of voters to understand the issues, recall their decisions, and actually carry out their intentions, and a given technology affects which ballot designs can be implemented. For example, voting systems based on touchscreen technology may be subject to frequent interface modifications that create a difficulty for election officials and voters but also make possible rapid prototyping for ballots and responsive redesign for error correction.

Vendors have the responsibility of enabling jurisdictions to define ballots. The specific ballot definition capabilities provided to the jurisdiction are of considerable importance, because they can increase or decrease the likelihood of confusing, misleading, or even illegal ballots. (For example, a vendor might provide user-tested and validated templates for jurisdictions to use as a point of departure. Or vendors could provide local election jurisdictions with ballot definition toolkits that enforce usability principles as well as local laws and regulations, to the extent feasible.)

4-32. **How is provisional balloting managed?** Of course, election officials have the option of insisting that a provisional ballot be processed entirely offline. But a vendor may offer such capabilities online. Online provisional balloting raises a number of issues:

- *Segregation of provisional ballots from ordinary ballots*. Since a provisional ballot counts only if it is determined later to be cast by a person eligible to cast it, it must be separated from ordinary ballots.
- *Maintenance of voter secrecy*. Given that the provisional ballot must be connected in some way to voter-identifying information (so that the voter's status can be later ascertained), the potential for secrecy violation is manifestly obvious. What mechanisms are available to ensure that voter secrecy rights are respected?
- *Ballot selection*. More advanced electronic voting systems may seek to support vote-anywhere voting, in which a voter can present himself or herself at any precinct in the state, identify his or her home jurisdiction, and expect the correct ballot to appear on the screen at his or her voting station. How will this capability be managed?

4.2.3.3 Usability Testing

Usability testing is done through simulations and experiments as described above. In addition to the response time and error data derived from experiments, it is useful to get subjective data, either from questionnaires or from focus groups or both. But a primary lesson from human factors engineering is that the number of different ways machines can confuse people is far larger than one can imagine from even the most careful on-paper analysis. While experienced designers and careful on-paper analyses are important elements of human factors engineering, repeated cycles of realistic and intensive testing with a broad range of users and reengineering to reduce the likelihood of errors is absolutely essential to the process. A broad range would include people with a diversity of education, socioeconomic backgrounds, technical experience, literacy, and physical, perceptual, language, and cognitive abilities. Realistic testing includes environmental conditions that approximate those found in the polling place, including attendant chaos, noise, and time pressure.

To illustrate the kinds of unusual and not-easy-to-anticipate problems that occur in operational use, consider that a voter may need to switch the language of presentation in mid-stream. Quoting from the field notes of a member of the committee who was observing:

> [In observations of early voting for the 2004 General Election in Los Angeles County,] a young, female Asian voter was observed in a Monterey Park early voting location (Monterey Park City Hall, Community Room), on October 29, 2004, at approximately 12:30 pm (the final day of early voting in Los Angeles County for that election). This young woman asked one of the polling place workers for assistance using the voting machine, and she clearly began to have some difficulties with her ballot. Eventually, she requested assistance again, which involved two polling place workers, as she wished to change the language that the ballot was presented in from Chinese to English, in the middle of casting her ballot. Eventually, the polling place workers managed to switch her ballot from Chinese to English on the electronic voting device. This voter was timed as taking almost 24 minutes to vote, from start to finish; other voters at this same location were observed typically taking from about 5 to 7 minutes to vote using the same electronic voting machines.

It is thus reasonable to ask about the nature of usability testing and the range of users involved in such testing.

4-33. **What is the range of the subjects used in testing usability?** As a general rule, the broader the spread of demographic and socioeco-

nomic characteristics of the test population, the greater the likelihood that potential operational problems will be identified in advance.

4-34. **What is the error rate in capturing votes of any given system? How is that error rate determined?** A commonly used and well-accepted aggregate metric for this error rate is the residual vote, defined as the sum of overvotes and top-of-ticket undervotes (in which the voter indicates no choice for the most important contest on the ballot, and thus the ballot does not count as a vote). Overvotes are clearly errors, whereas undervotes are entirely legal and may reflect a voter's preference to refrain from voting in a particular contest. Nevertheless, because the top-of-ticket contest (e.g., the contest for president of the United States) is the most important contest, it is assumed that an undervote for that contest reflects an error on the part of the voter.[36] Note that because the voter's experience is determined by a combination of the voting system, the particular ballot layout, and the particular environment (e.g., ambient noise, lighting, time pressure), a realistic estimate of error rate is obtainable only by undertaking the measurement under circumstances that are very close to those that would prevail on Election Day.

4-35. **What are the submetrics of usability that are applied to evaluate and compare systems?** Usability is in general a multidimensional issue, and different voting jurisdictions may place different weights on the various dimensions of usability. For example, a rural jurisdiction serving a voter population that almost exclusively speaks English may well place lesser weight on usability metrics that relate to ballot presentation in languages other than English than would an urban jurisdiction serving a large number of language minorities. Residual vote is a useful aggregate measure of usability, but making specific usability improvements in a voting system requires a more detailed understanding of why voters overvote and undervote. Moreover, residual vote is a conservative measure of error, in that it does not capture voters who vote for a candidate other than the one they intended.

4-36. **To what extent, if any, do problems with usability systematically affect one political party or another or one type of candidate or another?** Usability problems that have a greater effect on a certain demo-

[36]To illustrate the use of residual vote as a metric for comparing the performance of different voting technologies, Henry Brady used residual vote to compare the performance of punch cards in 1996 to that of optical scanning in 2002 in Fresno County in California. He found that the residual vote dropped by a factor of about 4 as the result of changing voting technologies. See Henry Brady, *Detailed Analysis of Punch card Performance in the Twenty Largest California Counties in 1996, 2000, and 2003*, available at http://ucdata.berkeley.edu:7101/new_web/recall/20031996.pdf.

graphic group, for example, may work to the disadvantage of a particular party.

4-37. **How is feedback from actual usage incorporated into upgrades to currently deployed systems?** The ultimate in operational testing is experiences during Election Day, when voting systems get their maximal workout. Because it is virtually certain that some users will be confused and make errors with any deployed system, it is desirable to have some method for systematically capturing anomalous voter experiences and using information about such anomalies as a point of departure for future upgrades. Vendors and election officials should therefore go out of their way to seek information about voter problems with a given system rather than to ignore or, worse still, suppress such reports.

4-38. **How does usability testing incorporate the possibility that different jurisdictions may create ballots that are very different from one another?** Because the voter's experience at a voting station depends both on the underlying technology and the way the ballot is presented, it is important that usability testing be conducted across a range of different ballots.

4-39. **Who should conduct usability testing on specific ballots?** Because the ITAs are not in a position to evaluate specific ballots that jurisdictions may use, ITA qualification does not provide assurances about the usability of given ballot. Indeed, the soonest that a specific Election Day ballot can be made available is after the relevant primaries for that election. Thus, election officials must either conduct usability testing themselves, or engage some other party (parties) to do it. An obvious—though hardly disinterested—choice is the vendor. But there may be other parties available to perform such services on relatively short notice.

4.2.3.4 Education and Training

Voter education is challenging. Because many people vote only once or twice a year, they may well forget how to use the systems they used in previous years. Given the rate at which people change residences, some nontrivial number of voters in any given jurisdiction are likely to be first-time voters there, and because different jurisdictions make their own decisions about which voting systems they will acquire, some people will always be voting on unfamiliar equipment. Some devices for entering input, such as touch screens, can behave idiosyncratically in a way that is dependent on how a particular unit is calibrated. Finally, product upgrades from vendors may change the user interface, which would result in a different "look" and "feel" from election to election. This suggests that education or training will be necessary, at least for some (significant number of) voters.

Voter education materials must be comprehensible to a wide range of people, and so should be written so as to not require high levels of education, be available in multiple languages, have visuals that correspond closely to the systems and ballots in use, provide step-by-step instructions, and be available to nonsighted individuals.

4-40. **How long does it take a first-time user to become familiar enough with the system to use it reliably and with confidence?** As a rule, this question can only be answered by simulation and direct user testing.

4-41. **What kinds of educational materials should be prepared and distributed in advance?** Many organizations, both partisan and nonpartisan, provide voter education materials that illustrate how to fill out ballots. While these materials are generally oriented toward the specific choices that voters will make, information about the operation of the voting systems that will be used is likely to be helpful to most voters. Such information can be made available in many ways, notably in print and online. Nonpartisan educational materials in multiple formats (e.g., video cassettes, DVD, and online or Web-based) teaching how to operate the units can be available to voters at the polls prior to actual voting.

4-42. **To what extent are practice systems available for use before and on Election Day?** While good "paper" instructions would be helpful, actual hands-on experience and familiarity would make a world of difference for the voter in operating a voting station. The availability of a demonstration station, configured identically to the ones that voters will actually use, would allow voters who are uncertain about the mechanics of voting to practice ballot casting in a realistic fashion. Even if demonstrator stations are not available in every polling place, making a few available in convenient locations prior to Election Day would help.

4-43. **What voter assistance can the voting station itself provide to users?** Nothing in principle prevents the voting system from providing information about the mechanics of casting a ballot. For example, voting systems can prevent overvoting (voting for more than one candidate when only one selection is allowed) by providing an indicator that such a condition has occurred and preventing the user from making the ballot final until the problem is corrected. They can also warn the user if an undervote has occurred—that is, that the voter has not made choices for certain offices or propositions—by asking if the undervote was deliberate.

It is also possible to have an online help facility that a confused or uncertain user can invoke. Context-sensitive help (i.e., help that varies depending on where the user is in the voting process) is generally much more helpful than generic advice that the user must read and compre-

hend before finding what he or she needs. Note also that in the unfamiliar confines of the voting booth, with lines of other voters waiting, voters may feel pressure to complete their votes as quickly as possible. Such pressure increases the likelihood of errors and may reduce the willingness of some voters to use online help facilities.

4.2.4 Reconciling Security and Usability

For a variety of reasons, election officials often believe that security and usability are necessarily traded off against one another. For example, the tension between overaggressive purging and underaggressive purging of a voter registration list reflects this trade-off: Greater security (and reduction of fraudulent voting) is associated with overaggressive purging, while greater accessibility to the polls is associated with underaggressive purging. Maintaining privacy in the voting booth is a matter of security, while allowing another individual inside the voting booth to assist the voter is a matter of usability. And, security by obscurity is fundamentally dependent on a denial of access.

These contrasts illustrate a more general point—in the design of any computer system, there are inevitably trade-offs among various system characteristics: better or less costly administration, trustworthiness or security, ease of use, and so on. Nevertheless, in the design of electronic voting systems, the trade-off between security and usability is not necessarily as stark as many election officials believe. That is, there is no a priori reason a system designed to be highly secure against fraud cannot also be highly usable and friendly to a voter.

The reason is that the security and usability requirements are directed at different targets. The biggest threat to security per se is likely to come from individuals with strong technical skills who are working behind the scenes to subvert an election. By contrast, usability is an issue primarily for the voter at the voting station on Election Day. Because these populations are qualitatively different, efforts to mitigate security problems and efforts to mitigate usability problems can proceed for a long time on independent tracks, even if they may collide at some point after attempts at better design or better engineering have been exhausted.

This point also has implications for the testing and certification process. Specifically, because security and usability are in large measure not attributes that must be traded off against each other, different skill sets are necessary for a competent evaluation of security and usability. Thus, it cannot be assumed that experts in one area are necessarily competent to evaluate issues in the other.

5

Life-Cycle and Training Issues

5.1 THE LIFE CYCLE FOR INFORMATION TECHNOLOGY SYSTEMS

The initial decision to procure an information technology (IT) system is only one dimension of the life cycle of that system. In the lexicon of information technology, the "life cycle" of a system begins with its initial purchase or acquisition—that is, when the system is first delivered. Concurrently, people must be trained to use, operate, and maintain the system. Problems in operation are inevitably discovered, ranging from small software bugs to major design flaws—and many of these problems must be fixed. Fixing a problem involves development of a putative fix and then testing the fix to determine that the problem is resolved and also that no other problems are introduced. In principle, the fix—or, more properly, the complete fixed system—must be legally certified under state law before and in time for an election. Then the problem fix must be deployed to the entire installed base of systems. In addition, new capabilities are often desired by the user, and a vendor may develop upgrades to accommodate those needs; upgrades must go through the same process of development, testing, and deployment as do problem fixes.

One of the most important dimensions is the cost and effort associated with continuing operation of the system over its expected lifetime. A second is that the expected lifetime of an information technology system may well be much shorter than budget-constrained state and local governments would either expect or prefer—and the Help America Vote Act

of 2002 (HAVA) does not provide funding for continuing operations or system replacement. It is thus helpful to consider some of these other dimensions explicitly.

5-1. **What is the life-cycle cost of any particular electronic voting system?** The initial procurement cost of any information technology system is generally only a fraction of its total life-cycle cost, which also includes costs associated with operations, maintenance, upgrades, and training.[1] (Put differently, within a few years of initial purchase, many voting jurisdictions have found that other nonprocurement expenditures exceed the initial purchase cost.) Moreover, there is generally considerable uncertainty about estimating or even identifying collateral costs. For example:

- Extra work by employees with high-tech skills may be required to support elections staff or poll workers in the field.
- Necessary security measures and security audits may well increase costs.
- Skilled program and contract managers with IT experience are generally needed, but may not already be on staff in the purchasing jurisdiction.
- County or municipality employees already drawing salaries may be used instead of other poll workers, thus rendering their costs invisible.
- Training and education expenses for in-house IT staff to develop an understanding of a system in enough detail to make authoritative statements about a system's operational properties may increase costs.

In addition, costs beyond initial procurement can increase dramatically in later years if vendor support for the purchased configuration is not available. Over some period of time, it is virtually inevitable that this will be the case, either because the vendor will have made available upgrades to the initially deployed system and no longer supports that system, or in less common instances because the vendor has simply gone out of business. Note also that upgrades are not necessarily a positive thing,

[1]For example, various studies of the total cost of ownership of personal computers in a work environment suggest that acquisition costs are less than 20 percent of the total cost of ownership per year. Assuming a useful lifetime of 3 years, acquisition costs are well under 10 percent of the total cost of ownership over the entire lifetime of the system. See John Taylor Bailey and Stephen R. Heidt, "Why Is Total Cost of Ownership (TCO) Important?" *Darwin Magazine Online*, November 2003, available at http://www.darwinmag.com/read/110103/question74.html.

or more precisely, they generally come with both costs and benefits. Upgrades often fix problems but have also been known to introduce new (and unanticipated) problems.

5-2. **What assurances can a vendor offer with respect to long-term support?** Given that elections happen relatively infrequently, continuity of the election process is an important requirement. Purchasers of electronic voting systems (that is, states or local election jurisdictions) must have assurances that a vendor will be able to support those systems for an extended period of time. (Historically, voting machines have had lifetimes measured in decades, but it is likely that any information technology system will be obsolescent and thus hard to support and maintain in much shorter time frames. Consider, for example, that the World Wide Web is now only 10 years old, and even automatic teller machines are programmed for replacement on a 15-year life cycle.) Purchasers might thus be concerned about issues such as the following:

- The presence of a sustainable business model and adequate capitalization that will allow a vendor to stay in business over the expected lifetime of the equipment. A vendor that goes out of business is not just a problem for its investors or owners; it is also a problem for the jurisdiction, because such a vendor will no longer be able to provide equipment and software support.
- The presence of a proven quality assurance infrastructure that can support the systems being sold over their entire life cycle.
- The cost of switching vendors in the event that a vendor goes out of business or proves unsatisfactory in its contract performance. A well-known strategy of vendors seeking business is to capture a purchaser with low initial costs and technology that makes it difficult for the purchaser to switch vendors later on. Such a strategy makes a great deal of sense from the vendor's perspective, but it leaves purchasers more or less at the mercy of the vendor in the middle of the system's life cycle.
- Contract provisions that ease the transition to another vendor should such a transition become necessary. For example, performance bonds are a common practice in the voting systems industry,[2] but performance bonds are usually large enough to place significant barriers to entry for both existing companies and new entrants in the field. (A typical performance bond is a substantial fraction of the total

[2]A performance bond is issued to one party of a contract (in this case, the purchaser) as a guarantee against the failure of the other party (in this case, the vendor) to meet obligations specified in the purchase contract.

value of a contract—it may even be 100 percent of the contract—and it serves to incentivize the vendor to fulfill the terms of the contract and to enable the purchaser to find another vendor should the original vendor default.) Another practice is source code escrow, which calls for the deposit of source code files and appropriate documentation with a mutually trusted third party during and after the completion of the contract. In the event that the vendor becomes unable or unwilling to continue to provide service to the purchaser, the source code is released to the purchaser so that it can seek another party to assume the first vendor's responsibilities. Source code escrow is a common, even routine, commercial practice. However, this practice alone does not provide complete protection against the risk of vendor difficulties.

5-3. **What are alternatives to purchasing complete integrated voting systems?** Outright purchase of an integrated electronic voting system is only one procurement model. Two other models are leasing rather than buying the system and purchasing election services rather than owning and operating voting machines. The first model may entail greater cost over the long run, while the second raises many questions about the appropriateness and legality of privatizing essential government services. A third approach is based on the procurement of individual components of a system from separate vendors (or lessors) that are subsequently integrated into a functional system. Such an approach requires the development and promulgation of standards for data and program interfaces that allow different functional modules to interoperate.

5-4. **How difficult will it be to change vendors if the original vendor becomes unresponsive or too expensive?** Vendors have many incentives to capture the loyalty of a purchaser, because a loyal customer represents a steady and predictable income stream. But there are many methods for building loyalty. Some are incentives—by offering the purchaser various services and perks not readily found elsewhere, a vendor can build a more enduring relationship with the purchaser. Others are disincentives—by forcing the purchaser to pay certain costs if it wishes to change vendors, a vendor may be able to lock in the loyalty of the purchaser even if it would be in the interest of the purchaser to change vendors in the absence of such disincentives.

For example, if the vendor is the only source of expertise on the operation and maintenance of a system, the purchaser is necessarily dependent on the vendor for support. But purchasers who are highly dependent on a vendor for support tend to pay much more than if they have access to independent sources of expertise. In principle, a purchaser can develop such expertise in-house or can contract for it with third parties

other than the vendor. In either case, the utility of this expertise is greatly enhanced by having access to the source code of the software running on the system in question.

As a general rule, systems that are designed in accordance with widely accepted standards, in a modular fashion, and with clearly defined interfaces are easier to support and maintain in the long run, because other vendors can also design system components in the same way and thus increase the likelihood that those components will interoperate with system components already in place.

5-5. **What logistical and administrative issues arise regarding the physical management of a voting system?** Election officials are responsible for the physical handling of machines before, during, and after an election, and different kinds of equipment have different handling requirements. For example, some systems require storage in climate-controlled environments. For subsequent auditing purposes, electronic records (e.g., flash memory cards) may require storage. Paper records must be stored in fire-resistant containers; how should flash memory cards be stored? Electronic equipment is typically more delicate and fragile than nonelectronic equipment—what procedures need to be followed in moving units between their storage locations and polling sites?

5.2 POLL WORKER TRAINING

Perhaps the most significant training issue that arises with electronic voting systems is the one associated with poll workers. Poll workers play an essential role in the electoral process today. Poll workers are individuals who assist with the polling process essentially on a volunteer basis (they are usually paid a token amount for their work on Election Day and for being trained, but in no sense can the job of poll worker be regarded as a significant income-producing job).

Poll workers have many responsibilities on Election Day, including the following:

- Physically setting up the voting site on Election Day (placement of tables and the like),
- Turning on the individual voting stations being used before the polls open,
- Resolving problems with voting stations if such problems arise during polling hours,
- Checking voter registration and acting as gatekeeper for voter access to individual voting stations,
- Answering any questions that voters may have about the mechanics of voting, and

- Ensuring that ballots (or totals) are delivered properly to the tabulation authorities.

Box 5.1 describes the experience of an actual poll worker in the 2004 election to provide some on-the-ground context for the realities of poll working. As obvious as the point is, it is sometimes forgotten that it is this myriad of on-the-ground experiences that shape the perceptions of ordinary citizens regarding an election.

In the context of electronic voting systems, the range of things a poll worker might be responsible for doing in each of these categories is arguably even larger than when nonelectronic systems are used. This is not to say that every poll worker will necessarily experience a wider range—only that he or she must be trained to handle a larger number of contingencies. In general, poll workers must know how to use the systems at least as well as any voter would need to know, and they must know still more than that, because they will be the first line of assistance for voters who are confused about how the system works. Poll workers must know enough about the system in use to be able to recognize a problem that arises at a voting station, and then to take action to correct the problem.

Against this backdrop, some important training questions arise:

5-6. **What is the nature and extent of the training required to make poll workers sufficiently knowledgeable about an electronic voting system?** The nature and extent of needed training depend significantly on the design and capabilities of the voting system in question. As a general rule, a system with greater functionality and that customizes its interactions to a voter's needs will require more training.[3] Poll workers may also need some knowledge about how to set up a voting station. For example, a voting station may need to be rebooted after it suffers a system crash, and a poll worker may be the only one available to do so promptly.

A useful benchmark might be a comparison with the training required for poll workers prior to the introduction of electronic voting. If a significant amount of additional material must be covered in the same training time, training problems might be reasonably expected, especially if there are changes from year to year in operating procedures and interfaces (as is often the case with IT-based systems).

New media for training, such as DVDs, videocassettes, and online Web-based education, may provide more complete poll worker training than has previously been possible.

[3]Examples of customization include presentation in different languages, use by persons with disabilities, and ticket versus individual choice voting.

Box 5.1
An On-the-Ground, First-Person Report of a Poll Worker

I [Leslie Sussan, Montgomery County, Maryland] served twice as an election judge in Maryland, first as an assistant chief judge in the primary and then as a check-in judge in the General Election. My experience was that goodwill and good intentions were plentiful. Still, problems with the quality of the training, the conditions we had to work under, and the unintended effects of the voting systems themselves were very evident.

Weeks before each election, election judges attended a mandatory 4-hour training session and were given a binder with instructions. The training sessions tended to highlight the many changes from the preceding election rather than proceeding through exactly what to do at each step. The effect was like the old joke of a native instructing a tourist to turn left where the red barn used to be. The first training I went to was almost all lecture, with only about 30 minutes' practice with an actual voting machine we saw for the first time. The second training devoted more time to role plays, but the presentation of what to do was fast and cursory, and most people had not read the manuals beforehand, resulting in lots of confusion. Little effort was made to explain the purpose of particular documents or requirements; the rush to get through "what to do" left no time for "why." The inadequacy of the training was evident when election judges tried to use their common sense to fill in the gaps in their memory and understanding. Check-in judges would ask to see identification from all voters, for example, because doing so seemed self-evidently reasonable to them. Yet, the law clearly required identification only from certain first-time voters. The judges at my precinct argued over when to give provisional ballots, because the guidance from the Board of Elections had changed between the two elections.

Most of the election judges were at or well past retirement age. We were basically amateurs, rather than trained professionals, and were paid only a token amount. We met at the poll the night before in order to set up some materials that could be prepared in advance and in order to meet the "team" for the first time. On Election Day, we had to arrive by 6:00 a.m. and were not permitted to leave the premises at all until the election was completed. The polls closed when the last person in line at the end of the voting period finished voting, and the procedures to shut down the polling place and secure everything took until 10:00 p.m. It does not take much imagination to understand how easily errors could occur with people in their sixties, seventies, and eighties working for 14 to 16 hours straight (after working on set-up the night before as well) with few breaks and little food.

During the day, we were supposed to be allowed occasional breaks to eat food we had brought in, while the chief judges substituted so as to maintain one election judge from each party at each station. This worked fine during the primary, but the high volume at the general election made it very difficult to keep the stations fully manned when the chiefs had to perform their other responsibilities too, such as handling provisional voters. Breaks became brief and rare, and some-

times single individuals tried (improperly) to keep lines moving while substitutes were juggled. Also, I was the only Spanish-speaking judge in a heavily immigrant precinct, and in the general election I often was called away from my post to translate (particularly because, although ballots were provided in Spanish, the audio versions available for blind or illiterate voters were not in Spanish and I had to read the ballot through for two voters).

We had an amazing number of forms, checklists, tallies, and documents to maintain and double-check. So, the check-in judges were supposed to find a voter's name in a voter registry listbook; find a matching voter authorization card (known as a VAC, a term unfortunately also applied to another document in the process) in a box; get signatures on both and initial them; make a mark on a running tally of the number of voters checked in by party registration; prepare an electronic plastic voting card; and send the person to the voting unit judge. The number of signatures in the log, VAC cards, and marks ought to all correlate. Then, the voting unit judge takes the voter to a machine; notes the number of the machine on the VAC, marks a running tally sheet on the machine; verifies that the electronic card pulls up a ballot properly; and returns the used VACs to the check-in judges. The number of marks on the tally sheets should match the electronic record in the machine of how many votes were cast on that machine. But every redundant record offers more opportunity for inconsistencies. A check-in judge who did not see the point of the tally by party in a general election focused instead on getting the line moving. A voting unit judge walked a voter to a machine and began to record the number of the machine on the VAC, when the voter asked a question. After answering the question, the judge showed the voter how to put in the plastic card and get a ballot and then tried hopelessly to remember whether or not she already marked the tally sheet for the machine.

The biggest complaint by voters was the interminable waits, and most of all the apparent inequity because some segments of the alphabet seemed to have much shorter lines than others. The segments of the alphabet were set up in advance to provide for the number of pairs of check-in judges assigned to the precinct. Preprinted signs were set up for each line (say, A-G, or L-R), and the bound registry list books were divided into the same groups as were the boxes of VAC cards. It was impossible to readjust on the spot when it became clear that the voters turning out did not fall evenly into the assigned divisions, because the list books could not be disassembled. Binding the books reduces the risk of tampering by adding or removing pages, but the binding could be done by individual letters to allow some flexibility. The check-in judges were the ones whom the voters blamed.

I would serve again, and there was something heartwarming about so many very ordinary people working so hard to make an election happen, but there was also quite a bit that was disturbing about seeing the sausage-making close up.

SOURCE: Leslie Sussan, Montgomery County, Maryland.

5-7. **How will election officials know that a poll worker has been adequately trained?** As procedures become more complex and the possible contingencies more varied, an assessment of a poll worker's knowledge may become necessary before he or she is selected to work at the polls (recognizing that requiring potential poll workers to undergo an assessment may well intimidate or discourage some of them from volunteering at all). A related issue is how the poll worker himself or herself will know about the adequacy of training. Poll workers who are conscientious may well be uncertain about various aspects of problem resolution and will want to know how to remedy those gaps in knowledge.

5-8. **How will poll workers get help when unanticipated questions or issues arise?** Almost independently of the training that a poll worker receives, it is virtually assured that some poll workers will encounter unanticipated problems during Election Day. Thus, some mechanism must be available to provide poll workers with assistance on a timescale that does not significantly interfere with the voting process. When these problems involve the operation of voting stations, the help mechanism will most likely be the responsibility of the vendor.

5-9. **What is the nature of the help mechanism(s) provided by the vendor?** Help mechanisms can take a variety of forms, and all may be relevant to a given situation. Vendors may provide documentation (e.g., sets of frequently asked questions) to help facilitate problem resolution, provide answers over a help line, or provide in-person support at the polling place. However, consider the following:

- For complex systems, documentation cannot be both comprehensive and easy to use. Furthermore, users must generally have some familiarity with the system in order to use documentation effectively.
- Though help lines can be quite effective in resolving simple problems, it is often difficult for a help line specialist to diagnose and provide advice on a more complex problem, especially when the specialist cannot see the station with the problem and the poll worker must describe the problem in words.
- In general, in-person assistance cannot be provided as rapidly as when help lines are used (assuming that help lines can handle peak call volumes). Also, though in-person assistance is usually the most efficacious method for problem resolution, it is also the most expensive and generally the least timely (because an individual must be dispatched to the appropriate location).[4]

[4]In at least one locality in the 2004 election, a vendor put a very large number of field technicians on call to provide prompt service. If this was part of its contract with the locality in question, the question arises as to whether the contract provides for such staffing for the

- New technologies, such as chat rooms or instant messages, may provide new channels for responsive assistance.

5-10. **What consequences flow from any vendor inability to provide adequate problem resolution on Election Day?** Given that the vendor provides various assurances that its systems will be usable on Election Day for voting purposes, it is reasonable to ask about the strength of those assurances. For example, the vendor might be required to post a performance bond that is forfeited if a certain level of problem resolution is not attained (e.g., forfeited if more than 5 percent of help requests cannot be resolved in 30 minutes).

5-11. **How can local election officials attract and ensure an adequate base of volunteers who can cope with the challenges of new electronic voting systems?** Problems of poll worker training may be exacerbated by the demographics of poll workers extant in many jurisdictions, where they are often individuals without much experience with technology.

lifetime of the systems in use or whether such staffing was intended as a "loss leader" to provide reassurances for other prospective buyers. If it was not part of the contract, the question arises as to the vendor's inclination to provide similar levels of support in the future.

6

The Broader Context of Electronic Voting

6.1 THE END-TO-END NATURE OF THE ELECTORAL PROCESS

In practice, public debate over electronic voting has devolved into an argument over the technical security of voting systems and whether or not a paper trail to facilitate election auditing is or is not desirable from a public policy perspective. While these issues are important, there is a broad range of end-to-end issues, from the point of capturing the voter's intent to assuring an accurate final tabulation of votes. Consideration of electronic voting cannot be divorced from these issues, which frame such consideration and embed it in a larger context. Furthermore, these issues are themselves embedded in a larger electoral system that includes voter registration databases, election planning and administration, procurement of election systems, and so on.

Put differently, challenges to election quality cannot be tied to just one potential problem whose solution would result in a near-perfect election process, but rather are the result of the cumulative impact of many potential failures large and small, including human error, equipment failures, procedural miscues, and so on. Thus, issues of the security or accuracy or usability of electronic vote systems have to be examined in the context of the entire electoral process. While the two previous chapters have addressed questions that election officials might reasonably pose in the course of deciding whether and how to move toward electronic voting, this chapter discusses this larger context in which electronic voting is

embedded and poses some questions that are essentially research questions with particular relevance to voters and elections past and present.

6.2 DATA ISSUES

Data are lacking on many aspects of the electoral process that are needed to make improvements or to conduct audits. With high-quality, consistent data in hand, a great deal more can be learned about the workings of voting machines, voter registration systems, and reforms in different states that would inform the election administration process. For instance, it would provide a basis for security assessments and transparency evaluations. Collecting data on incident reports could enable a feedback loop for election officials to prevent problems from occurring in other jurisdictions in real time; it could also facilitate forensic analysis to prevent problems from recurring after Election Day. Additional data on why registered voters did not reach a changed polling location, such as for reasons of greater distance or lack of information, could also help to inform questions related to the consolidation of polling places or future attempts at "anywhere" voting that would enable a voter to cast a vote at any precinct location.

Note also that because voting is a decentralized affair, with localities administering their own elections on their own systems, data must be very fine-grained as well as systematically collected to be most useful.

6-1. **What is the relative contribution of different sources of error in converting a voter's ballot intention to a final tabulation of votes?** For example, one might distinguish between voter registration errors that prevent a voter from voting, casting errors that result in votes being cast in a manner other than that intended, machine errors that record votes inaccurately, administrator errors that result in recorded votes being counted more or less than once, security problems that result in the deliberate commission of fraud, and so on. How do these sources of error differ with in-person voting, absentee voting, and provisional voting? Historically, voter registration problems have been the most significant source of problems (including fraud) in voting, regardless of the voting technology used.[1]

6-2. **What data collection must be mandated by states?** Data collection regarding elections is an inherently local process, but the very localities with persistent election problems often do not have strong incentives to collect data that might document the existence of their problems. Thus,

[1]Caltech/MIT Voting Technology Project, *Voting: What Is, What Could Be?*, July 2001.

the states may have important roles to play in ensuring that appropriate data are collected systematically in all jurisdictions.

6-3. **What data are needed to evaluate the performance of electronic voting systems?** Because electronic voting systems are relatively new, even localities that have been collecting lots of data for a long time will need to adjust their data-collection practices. While certain types of data continue to be relevant (e.g., number of individuals turned away from the polls for improper registration), other data types are relevant only to electronic voting systems. For example, the number of times that a voting station needs to be rebooted or the time a system is unavailable for voter use only have meaning in the context of an electronic voting system. Other data may be necessary to evaluate how voters view electronic voting systems. For example, it may be useful to compare the number of people who come to the polls versus the total number of ballots cast on electronic voting systems. This comparison might shed light on the number of people who try to vote on electronic systems but fail to actually push the final button that records their ballot. (See also Box 4.6.)

6.3 PUBLIC CONFIDENCE IN ELECTIONS

Election officials have been very concerned that various election problems in recent election years (most particularly in 2000, and to a lesser extent in 2002 and 2004) have shaken public confidence in elections, with the likely impact of depressing voter turnout in the short term and potentially undermining the legitimacy of government in the longer term. They have further believed that the controversy over electronic voting could have a negative effect in this regard in the jurisdictions that use electronic voting, a point of particular significance when margins of electoral victory are very small. Electronic voting skeptics have argued that some wariness regarding untested and unproved electronic voting systems was justifiable. The introduction of new technologies into the polling place may help to draw in people previously disinclined to vote, or it may erect barriers, real or perceived, to broad voter participation. Furthermore, these impacts may differentially affect different demographic groups.

6-4. **What are the factors that influence public confidence in elections?** What is the relative contribution to such trust of various factors, including faith in specific public officials, trust in the democratic process, personal experience at the polling place, lack of public controversy, broad acceptance by societal elites, the substance and tone of election and political rhetoric, technological literacy and knowledge, voting system ease of use, the reality or appearance of partisan election officials, the level of spending on elections, the tone of campaign rhetoric, and the presence or

absence of public arguments about voting systems? What factors specific to elections contribute to public confidence (e.g., the outcome of the election;[2] the transparency of the process, the availability and frequency of recounts;[3] the management of the election by nonpartisan election officials; and so on)? In this light, it is clear that voter confidence in elections is multifaceted, and a voter's experience with the technology of voting per se is only one aspect of it. All of these factors, and no doubt others, will interact to influence voter confidence.

Nor is it entirely clear that all of these factors are well defined. Election outcome and frequency of recounts are reasonably clear, but what precisely is the meaning of election transparency? By one definition, it involves posting of as much information as possible on the Internet and elsewhere about election results, having observers who can watch voting and vote tabulation, having observers watch the loading of software and perhaps watching those who are guarding machines. Others might argue that only when the source code of electronic ballot marking and tabulation systems is public can an election be transparent. Still others would say that the mathematics underlying the system must be readily comprehensible.

That said, it is still worthwhile to develop voting systems that promote confidence, and voting experiences that leave the voter uncertain or frustrated are unlikely to do so. Tapping into voter sentiment immediately after an election (rather than waiting a long time afterwards) will generate anecdotes and recollections that are more likely to be accurate and undimmed by time. Interviews, voting simulations, exit polls, and

---

[2]Richard Hasen notes that in 1996, about 9.6 percent of the public (7.5 percent of Democrats and 12 percent of Republicans) thought the manner of conducting the most recent presidential election was "somewhat unfair" or "very unfair." In 2000 (after the November election), the number jumped to 37 percent of the public (44 percent of Democrats and 25 percent of Republicans). By 2004, 13.6 percent of the public had strongly negative views of U.S. election administration (21.5 percent of Democrats and 2.9 percent of Republicans). These patterns were reversed in Washington State in the aftermath of the 2004 gubernatorial election, in which a Democrat was declared the winner after a series of recounts and court battles. In a January 2005 Elway Poll of Washington voters, 68 percent of Republicans thought the state election process was unfair, compared to 27 percent of Democrats and 46 percent of Independents. (Richard L. Hasen, "Beyond the Margin of Litigation: Reforming U.S. Election Administration to Avoid Electoral Meltdown," to be delivered at the 2005 Annual Meeting of the American Political Science Association, September 1-4, 2005, and forthcoming in *Washington and Lee Law Review* 62 (2005). Some similar data from the American National Election Study of 2000 can be found in Henry Brady, "Trust the People: Political Party Coalitions and the 2000 Election," in *The Unfinished Election,* Jack Rakove, ed., Basic Books, New York, 2001.)

[3]For example, a philosophy adopted by some states regarding recounts is to make them as inexpensive as possible and to reduce barriers to undertaking recounts to the minimum level possible, on the theory that this practice promotes public confidence in elections.

focus groups all have a role in understanding voter confidence. Finally, special care must be taken to understand the concerns of voters with disabilities or voters who come from language, ethnic, or racial minorities.

6-5. **How do confidence in and knowledge about elections and voting mechanisms vary across demographic groups?** Different demographic groups perceive technology and social processes in different ways, and there is no reason to expect that this is not true with respect to their perceptions of elections and voting systems as well. For example, the introduction of electronic information technology into the polling place may help to draw in people previously disinclined to vote, or it may erect barriers, real or perceived, to broad voter participation. Understanding how these new technologies (and the publicity regarding their introduction) may affect the nature and extent of voter turnout among different demographic groups is likely to be of interest to election officials.

6-6. **What would be the impact on voter confidence of giving independent observers the ability to audit or scrutinize the conduct of an election?** In the past, voters had to rely on muckraking sources, on parties, candidates, or the press to raise questions about the integrity of an election, and to obtain the data needed to support allegations of election impropriety. But a number of new information technologies can put at least some of this power in the hands of the general public. For example, David Chaum has demonstrated that the use of appropriate cryptographic mechanisms enables a voter to cast a vote in perfect secrecy but still be able to check that his or her vote was actually counted in the total count for a given candidate,[4] though the specific mechanisms involved are far from transparent. Public disclosure of voting system source codes may help to promote vendor accountability and reassure those concerned about security, but might in some cases also compromise trade secrets that competitors could exploit or expose security vulnerabilities that adversaries could exploit. An analogy in this regard is the requirement that donations to a particular political campaign in excess of a certain amount must be listed publicly.

6.4 TESTING, CERTIFICATION, AND EVALUATION

As noted in earlier chapters, the process of testing and certifying electronic voting systems is complex. Yet states and local jurisdictions rely on testing and certification for indicators of whether a system is safe or unsafe to acquire. Today, the process is based on federal qualification and state

[4]David Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections," *IEEE Security and Privacy* 2(1):38-47, January-February 2004.

certification. But the qualification and certification process is cumbersome and slow and potentially subject to certain conflicts of interest.

6-7. **What are alternatives to the current testing and certification infrastructure?** The Independent Testing Authorities (ITAs) are private entities, designated by the National Association of State Election Directors and its successor, the Election Assistance Commission, to serve that role. Vendors contract with any ITA with whom they can negotiate an acceptable contract. Although there are no credible allegations of misconduct to the committee's knowledge, the possibility that a vendor might receive a "sweetheart" evaluation from an ITA is an obvious one to consider under these circumstances, especially because there are multiple ITAs all vying for such business. Possible alternatives are addressed in Box 6.1.

6-8. **Who will conduct testing that is needed beyond what is required by the qualification and certification process?** Neither the qualification nor the certification process addresses problems that might arise in actual operational use. In actual use, some voters are likely to encounter frozen screens that refuse to accept input, jammed printers, improperly printed scan sheets, and so on. Allegations of machine rigging will arise. Some impartial and unbiased party, with the requisite technical knowledge, must be able to investigate these problems (both real and alleged) if citizens are to have confidence in election outcomes.

6-9. **What certification requirements, if any, should be imposed on statewide voter registration systems?** Voter registration systems are highly customized to the needs of individual states and are thus developed in close cooperation with state election officials. Inasmuch as certification ensures that a certified system meets a minimum set of functional and performance requirements, certification of voter registration systems could impose a greater degree of uniformity on voter registration practices across states. Whether this is desirable or undesirable almost certainly depends on the point of view of the person making the judgment.

6-10. **How will election officials respond if, after all is said and done, voters use voting systems that are running uncertified software?** The combination of immovable election dates (general election or primaries), relatively slow qualification and certification processes, and relatively immediate needs for software updates to correct software bugs or accommodate new legislative mandates virtually assures that some jurisdictions using electronic voting systems may wish to use software that has been patched or altered to fix pressing problems but has yet to be recertified for use. In the best of all worlds, election officials would be able to demand—and obtain—from the vendor a formal notice that all certification and qualification requirements were met. But in the real world, the

Box 6.1
Possible Components of an Institutional Infrastructure to Support Electronic Voting

The list below suggests some of the functions that this infrastructure might support and possible mechanisms for how these functions might be served. The committee expresses no view on the desirability or undesirability of any of these mechanisms, except for comments made in the main text.

Research and Development

Research and development (R&D) on electronic voting systems would support future improvements in such systems by building an open knowledge base accessible to all vendors and would-be vendors in the field. (In principle, R&D can be proprietary as well as public; in practice, it does not appear that large firms are entering into the electronic voting systems market, and small firms are generally unable to sustain research over any extended period of time. Thus, some kind of public support may be necessary to undertake significant R&D.) Note that "research" would include both technical and nontechnical work, the former devoted to improvements in the systems themselves and the latter devoted to better understanding of the environments in which electronic voting systems are used. Alternative models of support include:

- Intramural or extramural federal program (National Institute of Standards and Technology? Department of Justice/National Institute of Justice? National Science Foundation? U.S. national laboratories?),
- Private-public partnership analogous to Sematech,
- Research funded in accordance with the U.S. Department of Argiculture's Agricultural Extension model, and
- Regional R&D consortia (funded by states with similar electoral needs).

Qualification and Certification

As noted in the text of the present report, qualification and certification provide some degree of assurance to purchasers that the systems meet certain standards. But when testing authorities compete against each other for business, a vendor can select the authorities most favorable to its products or negotiate for

realities of software development against fixed deadlines mean that time is limited, and election officials may be faced with two unpalatable alternatives—not fixing a problem or fixing it with uncertified or unqualified software. (Vendors are also likely to argue that the fix is not "large enough" to warrant recertification, as discussed in Section 4.2.2.3.)

This same question applies in a different form to the entire standards and certification process. That is, the standards-setting process is time-consuming, and thus new issues are likely to arise during that process—

advantageous testing procedures. Whether or not this actually happens in practice is not as important as the fact that there is no real way to know whether it does happen. Alternative models include:

- Federally chartered center based at U.S. national laboratories,
- State/regional centers based at state universities (e.g., Kennesaw State model for Georgia),
- Underwriters Laboratories model, and
- State-funded nonprofit organization (analogous to Consumers Union).

Field Investigation and Testing

A hard-won lesson learned from much information technology experience is that the investigation of anomalies is greatly enhanced by the preservation of as much of the state of the machine(s) as possible at the point of the alleged malfunction. In practice, this means that the system should be taken out of use and power maintained so that important information in memory is not lost or that a memory map should be taken before powering down. All relevant records should then be made available to the vendor and to an independent body for subsequent investigation. Parallel testing on randomly selected machines deployed to polling places is also an important function that can provide statistical reassurance that machines deployed are functioning as expected. However, no mechanism exists today for ensuring that these functions are performed when anomalies and allegations of fraud in electronic voting systems arise. Alternative models for an independent body include:

- A federal body analogous to the National Transportation Safety Board, and
- State or regional bodies analogous to the National Transportation Safety Board.

These bodies could also be empowered to receive reports of voting system irregularities that intentionally bypass election officials on the chance that these officials might have had some responsibility for these irregularities or some incentive for covering them up. This approach is based on lessons learned in the financial industry, which underscore the importance of upward communication routes that bypass an entire chain of administrative command en route to an outside independent audit committee.

with the result that the standards may well lack relevance to the current context when they are released. Certification processes presume the stability of an artifact for evaluation, but artifacts evolve as new problems and needs are uncovered. Thus, the updated version of a product may well be uncertified in time for use in any given election.

Finally, to the best of the committee's knowledge, there are no penalties or liabilities associated with the use of uncertified election software, even when state election law requires the use of certified software.

As for evaluation, the concept is broader than certification, which in a strict sense assesses the compliance of a system with a given set of standards. Evaluation also includes notions such as fitness of purpose. Today, private sector vendors drive the design and configuration of the electronic voting systems they offer for sale. For obvious and understandable reasons, these firms are highly motivated to develop systems whose sale will maximize their profits. Such an approach begs the question of whether less expensive systems might still be suitable for large-scale voting use. Few mechanisms exist today to undertake such evaluations systematically; the institutions for R&D and for certification and qualification described in Box 6.1 might serve such a function.

6.5 FUNDING AND SUSTAINING IMPROVEMENT

Aggregated over all jurisdictions and as a rough average, election administration costs the states about a billion dollars per year, regardless of year and prior to the passage of the Help America Vote Act of 2002 (HAVA), of which a very small fraction is for procurement of equipment.[5] Appropriations for HAVA have added significant sums (several billion dollars) for the procurement of new voting systems, but HAVA was never intended to assume an ongoing federal role in supporting and operating these systems. Nevertheless, the ongoing maintenance cost of a system is in general much larger than its initial acquisition cost.[6] Systems need to be upgraded as more is learned about their suitability for use and about the problems they encounter. And costs of election administration are likely to rise in the future as the result of mandates such as those contained in HAVA.[7] These points raise questions about long-term sustainability.

6-11. **How will funding be provided for the periodic refreshment of electronic voting systems?** Electronic voting systems will either have to be replaced periodically or expertise and spare parts will have to be maintained for an artificially long time that is not market supported—either is expensive. How will funding be made available for technology refreshment on a timescale comparable to the obsolescence time of electronic voting systems that are deployed today? How will equity of access

[5]Caltech/MIT Voting Project, *Voting: What Is, What Could Be?*, July 2001.

[6]See Footnote 1 in Chapter 5.

[7]For example, HAVA directs the states to create and maintain centralized databases for voter registration but does not authorize appropriations for this mandate.

to electronic voting systems be maintained across local election jurisdictions with disparate financial resources?

6-12. **How will research and development on electronic voting systems be supported and performed?** Over time, electronic voting systems will improve, just as other information technology (IT)-based systems have improved. But such improvements draw on an underlying R&D base. For electronic voting systems, some improvements are likely to piggyback on improvements in generic information technologies. (For example, advancements in cryptography and cryptographic applications may help to address concerns about security of voting. Human factors and user interface research may be useful in the design of electronic voting systems. Work on the design of dependable computer systems may help to improve the reliability of electronic voting systems.) But other improvements will depend on the availability of specialized knowledge that can be obtained only by examining electronic voting systems in particular. Thus, some mechanism (perhaps involving a mix of public and private funding or perhaps one or the other exclusively) will need to be found to support and sustain such research. As for the appropriate level of R&D investment, the committee observes without comment that information-intensive industries in the private sector typically spend about 10 percent of their gross revenues in R&D activities of various sorts. If election administration is regarded as an information-intensive enterprise, R&D investments of about $100 million per year might be expected. Who will perform the research is a second question (see Box 6.1).

6-13. **What is the impact of evolving standards on deployed electronic voting systems?** Standards for all technologies invariably evolve over time as more is learned. Indeed, R&D would be useless if it were not ultimately reflected in the standards to which certified or qualified systems must conform. But standards evolution will almost certainly result in some previously certified or qualified products being in violation of some part of the new set of standards. In the analogous situation in building codes, changes in building codes generally only apply to new construction, whereas regulators in the gambling industry are willing to decertify gambling machines previously deemed in compliance with the old standards. Election officials must decide how to proceed in this situation.

6-14. **What are the incentives for and barriers to improving electronic voting systems?** The ultimate consumer of an electronic voting system is the voter. However, the system vendor is not ultimately responsible to the voter, but rather to the locality that purchased the system. In principle, the locality is a governmental agency that is responsible to the voter, but in practice the purchasing entity must make significant efforts to stay in touch with and be responsive to the concerns of individual voters. Thus, taking into account the inevitable improvements in the

power and capability of information technologies (both hardware and software), a careful analysis of incentives and barriers would do much to shed light on the rate and nature of progress that electronic voting systems will undergo in the future. Note also that improvements in the technology of voting are not the only (or even necessarily the most important) improvements that can be made—election procedures and organization are also possible areas of improvement for many states and local election jurisdictions.

6-15. **What lessons learned relevant to electronic voting can be found in other regulated industries (e.g., gambling, finance) and government?** Computer scientists who have examined electronic voting often argue that voting systems are unique in their needs and requirements. This is surely true in certain ways (e.g., the need for absolute user privacy and the need for auditability rarely coincide in any other application). In fact, however, other industries have faced and addressed many of the same challenges.

For example, modern gambling machines are controlled through an embedded microprocessor that must be programmed, and the gambling industry (as well as government regulatory bodies) has developed techniques to guard against the possibility that a machine might be programmed improperly so that its payout is something other than that promised to the consumer. Both banking and the gambling industry have relevance to elections in that all share similar requirements for auditability and usability by people of diverse backgrounds. What can be learned from experiences in those other industries or sectors with respect to regulation, administrative rules, and contracting? Box 6.2 describes some possible lessons learned from the gambling industry.

Also, regulatory and investigative models from other industries might be helpful. For example, some have advocated a standing body whose role is to investigate statistical and historical anomalies in the outcome of an election, allegations of fraud, system failures, and other incidents involving electronic voting systems in much the same way that the National Transportation Safety Board investigates every plane crash in the United States. Such a body would address a very broad set of issues that might be relevant. These advocates believe that this kind of independent oversight could improve security and enhance public confidence by quelling unfounded concerns and rumors.[8]

[8]An important element of aviation safety in the United States is the Aviation Safety Reporting System, under which information contained in or derived from properly submitted reports of incidents potentially related to aviation safety or the violation of Federal Aviation Administration regulations cannot be used in any disciplinary action, except in cases of criminal offenses or accidents. By analogy, a standing body on voting systems might invite anonymous reporting of mistakes, and treat these reports as opportunities to learn rather than initiate action against culpable parties.

Box 6.2
Lessons from the Gambling Industry

Slot machines used in the gambling industry have many similarities to the systems used in electronic voting. In essence, both are computers, and it is important that they be accurate and reliable, both in appearance and reality. The state agencies responsible for regulating the industry have developed procedures and rules for ensuring that all participants (gamblers, casinos, and the state tax authorities) are treated fairly.

The parallels are far from exact, but it is worthwhile to consider some of the principles that the states have evolved to regulate gambling machines:

- Vendors of slot machines must be licensed.
- Standards govern what the machines may and must contain.
  —Standards are written clearly enough that compliance can be ascertained.
  —Independent testing of machines confirms or disconfirms that a given machine is compliant with the relevant standards.
  —Standards are updated on the basis of experience.
- Slot machines in the field are subject to random and routine compliance inspections.
- Authorities have a dispute resolution process in place to address disagreements between machine and gambler.
- Security is built on the assumption that some people will try to cheat (either users or slot machine operators).
- Software for slot machines is entirely controlled, from certification to insertion into machine.

Some of these principles may be relevant to the management of electronic voting machines. On the other hand, there are also substantial differences between the gambling and voting environments. From the point of view of the relevant technical requirements, gambling does not entail a presumption of privacy. Thus, slot machines can keep records of every action, and these records can be used along with in-person testimony for dispute resolution and auditing. From an administrative point of view, the finances are very different as well: state regulation and oversight of each machine costs several hundred dollars a year, paid by the casino. (With about 800,000 voting machines in use on Election Day, a similar cost imposed on voting machines would add about 10 to 15 percent to the nation's yearly expenditures on elections.) From a logistical point of view, slot machines are used every day, a characteristic that reduces the educational needs required of the user to operate the machine. And on-site maintenance is available, which minimizes the amount of time that a machine may be inoperative.

SOURCE: Briefings to the committee from Nevada and New Jersey gambling regulators, December 9, 2004.

6.6 ELECTION INSTITUTIONS

Nonelectronic voting systems have had a long history of operation, one measured in decades. Accordingly, election officials have not had to deal very much with issues of technological change. The introduction of electronic voting systems into the electoral process is thus potentially disruptive to that process. Perhaps more relevant is the fact that the timescales of change for information technologies is much shorter than decades, a point that raises the prospect of a more or less *continuous* disruption to the process. Consider, for example, that the interval between presidential elections is 4 years—in the world of information technology, 4 years is a very long time, and an electronic system used to process the presidential vote in any given year may never be the same in any subsequent presidential election. From the standpoint of a voter, the significance of internal changes in the underlying system can be minimized by concealing them behind a user interface that remains the same, much as Web browsing has remained more or less the same over a number of years despite many changes in the technology of browsers. Nevertheless, these internal changes may be significant from the standpoint of election officials, because (by definition) they change the behavior of the system—and may introduce unanticipated quirks of behavior that confound or confuse an internal administrative process. (Note that comments about rapid technical change apply to any new technology, including the retrofitting of newer technologies (e.g., paper audit trails) on top of new ones (e.g., direct recording electronic systems) not originally designed to accommodate those newer technologies.)

Such rapid change raises many issues for electoral institutions.

6-16. **How can election officials obtain sources of information about electronic voting systems other than the sources provided by vendors?** Vendors know a great deal about the systems they sell and, given the highly technical nature of electronic voting systems, have a significant information advantage over those making decisions about procuring or maintaining these systems. Moreover, vendors have strong incentives to be forthcoming only with information that is favorable and supportive of a decision to proceed. Election officials may wish to engage the services of others to help break this asymmetry.

6-17. With dramatic changes in the election environment, the law, public scrutiny, and technology, **how can election officials obtain the knowledge and information needed to respond to and manage change effectively?** These issues are particularly important in communities without full-time election officials.

6-18. **What institutional infrastructure is necessary to support cost-effective use of electronic voting systems over the long term?** Given the complexity of electronic voting systems and the revolutionary changes in voting and electoral processes that they are likely to enable, intuitions and common wisdom about what is possible that election officials and the public have built up over a century of conducting elections in the United States are probably an inadequate basis for understanding the full potential and risks inherent in these systems. Thus, it is important to consider how mechanisms might be established (see Box 6.1) to support research and development activity that would improve security, reliability, usability, and functionality in new generations of electronic voting systems; provide certification or other services that help election officials make informed decisions about products that they might purchase, lease, or use; conduct field testing and investigate reports of operational difficulty or other anomalies in the use of electronic voting systems; consider issues of electronically perpetrated fraud; and disseminate information about these systems on a nonpartisan basis.

6-19. **What do the equal protection requirements of voters enunciated in *Bush v. Gore* mean for decisions about voting technologies and their supporting infrastructure?** Traditionally, local election jurisdictions have controlled election administration and acquisition of voting systems. But *Bush v. Gore* found that certain jurisdiction-to-jurisdiction variations in the standards for determining voter intent were inconsistent with equal protection requirements. A variety of issues related to electronic voting may thus be implicated:

- Differences in functionality afforded by different electronic voting systems that may be acquired by different local election jurisdictions.
- Differences among local election jurisdictions in personnel training, administrative capacity, and the availability of professional staff needed to maintain and use electronic voting systems.
- Differences in the tax base and other resources available to local election jurisdictions for acquisition, maintenance, training, and education associated with new electronic voting systems.

Perhaps in response to the *Bush v. Gore* decision and HAVA mandates, many states—including Alaska, Georgia, Hawaii, Maryland, New Hampshire, Oklahoma, Rhode Island, and Vermont—have already adopted centralized statewide technology acquisition programs, though it is as yet unknown if centralized acquisition results in more uniform election administration across local jurisdictions.

6.7 THE ROLE OF THE PRIVATE SECTOR IN ELECTION ADMINISTRATON

Election administration has never been a function performed entirely by government. Indeed, private political associations (interest groups and political parties) have been involved in the administration of elections for a very long time. These private associations provided ballots under the ballot systems used before secret ballots were introduced. Further, as noted in Section 2.2, elected officials are associated with these private political associations.

Private firms have also been involved in election administration, a fact consistent with a trend over the last few decades of many local governments outsourcing certain functions that were previously managed and operated by those governments. There have been many reasons for this practice, including a belief that outsourcing will result in greater responsiveness and reduced costs. Various kinds of functions have been outsourced, including trash pickup, parking enforcement, and bus services. However, in certain instances outsourcing has created considerable controversy and argument over whether the particular function being outsourced should be outsourced—that is, whether a given function is inherently a function of government.

In election administration, private firms have for many years routinely undertaken certain election administration tasks such as the design, layout, and printing of ballots—a practice that generates little controversy. But local governments are also turning to private firms to provide electronic voting systems, to program them appropriately, and to repair and maintain them over time. Similar comments apply to many statewide voter registration databases. For both electronic voting systems and voter registration databases, vendors are often the primary and most important source of expertise, and gone are the days when the county or municipality had its own staff to repair and program its lever machines.

It is unknown whether the involvement of private firms improves election administration in some overall sense. In some states, the introduction of electronic voting systems (both direct recording electronic systems and optical scan systems) has increased dramatically the role of private firms. To the extent that private firms are involved in those aspects of election administration that relate to electronic voting systems, a number of important questions do arise, some of which cut across other areas discussed elsewhere in this report.

6-20. **What security concerns (Section 4.2.2) arise with the intimate involvement of private firms in the operation and maintenance of voting systems?** Are there reasons to suggest that security issues may be

more or less well managed by private firms than by local county or municipal governments? How should citizens or election officials determine if there is an "unhealthy" dependence of a local election jurisdiction on a given vendor?

6-21. **What are the roles of vendor certification and a code of ethics for vendors?** To date, the qualification/certification process has focused on the voting systems that vendors offer rather than qualifications of the vendor. In some other sectors, qualification of the vendor itself is also used as a selection criterion. For example, procurements may only be made from vendors whose business and development processes conform to some standard (e.g., an ISO 9000 standard). Acceptance of and conformance to a code of ethics can also be a requirement. The content of a code of ethics and a vendor certification requirement, as well as the roles that these might play, are questions that warrant further exploration.

6-22. **What would be the impact of consolidation among voting systems vendors?** A common path in any new niche is the initial proliferation of a large number of small vendors, followed by consolidation as weaker vendors drop out of the market. If this path is followed in the voting systems or election services market, a few large private firms will be in the position of managing and administering elections for a large number of local jurisdictions—raising the possibility that those who control these firms will be able to exert undue and improper influence on election outcomes for either financial or political reasons.

6-23. **How will contractual responsibilities be maintained over time?** As suggested in Section 5.1, the longevity of a private firm is not guaranteed. But an election jurisdiction that is strongly dependent on a vendor runs the risk that election services may be disrupted by discontinuities in support. Even if performance bonds are posted (a common requirement of acquisition contract, though disliked by many vendors), money is a poor substitute for continuity of service.

6-24. **Who owns the data associated with the holding of an election?** When governments are solely responsible for the conduct of an election, the ownership of the data is clear. (Box 4.6 indicates some of the data that might be in question.) But if private parties have a legitimate claim to the data, government officials are unlikely to have comparably unfettered access to that data, especially if such data might embarrass or compromise those private parties in some manner. For example, if election officials wish to audit an election to see where improvements are needed, vendors may be reluctant to share data indicating that their systems operated improperly.

A collateral question involves the ownership of the physical media on which data are stored. For example, vote totals may be recorded on a data memory card. If allegations arise that the card also contained executable

code that could have illegally affected the behavior of individual machines, access rights of auditors to the card itself may not be clear in the absence of a specific understanding about the media.

6-25. **Who bears responsibility for failures or irregularities in the election process?** When private parties play an integral role in election administration, lines of responsibility are less clear than when government is responsible for all significant aspects of election administration. And, to the extent that laws intended to ensure properly conducted elections are targeted at election officials, these laws may need to be updated to include private parties that have assumed certain responsibilities previously associated with election officials.

6.8 RESEARCH QUESTIONS

As the committee examined the issues, it became increasingly clear that much of the basic knowledge and information about voting and elections that one might hope had been codified does not exist or is not easily accessible. This section sketches out some of the relevant research questions that would help to inform election officials seeking to make good decisions about how to administer and manage elections in the context of new technologies that may enable new options for discharging their responsibilities.

6-26. **What new options (or variants on existing options) do electronic voting systems enable?** For example, electronic voting systems could support instant runoff voting (in which voters express a rank ordering of their preferences for a given race), so that races that require a majority (rather than a plurality) for victory need not require a second election for resolution. A second option is that the presentation of pictures of the various candidates for a given race is more easily managed with electronic voting systems. How might electronic voting systems improve or diminish the cost-effectiveness of alternatives to traditional voting such as absentee voting or early voting?

6-27. **How can electronic voting systems be made more secure?**

- Within the information technology world, there are many who advocate the use of open source code as a security measure. Others argue that disclosure of vulnerabilities is dangerous and facilitates attacks. What would be the impact on security of the disclosure of election system software (perhaps on a limited basis subject to nondisclosure)?

- How can voters be reassured that a vote cast in a certain way has indeed been counted that way in the tabulation?[9] Note that this question goes far beyond the question of a voter-verified audit trail, since such a trail only provides assurances that the vote was recorded as cast.
- Given that premiums on voter secrecy are high, what mechanisms might enable individual voters to give up some degree of secrecy in exchange for some degree of verified assurance that their individual votes are counted? Under what circumstances might such mechanisms be desirable?
- What are the known technical threats to the security of voting systems? How often have these threats manifested themselves? What is the likelihood of these threats? What are likely future threats?
- How do legal standards for proof and evidence relate to security requirements for voting systems? Note that the relationship is bidirectional. In one direction is the issue of how legal standards for proof and evidence affect security requirements in voting systems. In the other direction is how security considerations might affect legal standards and requirements.
- What indicators (statistical and otherwise) can be used to suggest where further investigations into the possibility of election fraud or error might be warranted? Statistical analyses and historical anomalies cannot prove that fraud or error has occurred but can point to possibilities worth investigating. Such approaches are analogous to methods used by the Securities and Exchange Commission to indicate the possibility of stock fraud or insider trading.
- How can the impact of technical vulnerabilities be mitigated by organizational or procedural measures? How can the impact of organizational or procedural vulnerabilities be mitigated by technical means? Though it is certainly a worthwhile endeavor to improve technology to reduce vulnerabilities, it is sometimes the case that the likelihood of exploitation of those vulnerabilities can be reduced as well. Consider, for example, that an audit (a procedural technique) can reduce the likelihood of improper programming introducing large errors into a vote count. Similarly, using cryptographic techniques to authenticate a flash memory card containing vote totals from a precinct can help to reduce the likelihood that a fraudulent flash memory card can be improperly substituted for it when precinct vote totals are delivered to the tabulation authority.

[9]Chaum's work, cited in Footnote 4, is a step in this direction.

6-28. **What are the operational implications of the voter-verified paper audit trail?** As noted in Box 3.2, much of the nation is moving forward with some form of paper trail requirement for electronic voting systems without an empirically based understanding of its actual impact on elections using direct recording electronic systems. Thus, it seems worthwhile to undertake empirical research on questions such as these:

- How can voter-verified paper audit trail (VVPAT) technologies be added to already complex electronic voting systems without adding to the burdens already placed on poll workers? As discussed in Section 5.2, poll workers are typically poorly paid (or serve as volunteers), are sometimes inadequately trained, may not be technologically savvy, and are often stressed.
- How do VVPATs impact the expenses of conducting and administering elections? On the one hand, they might increase costs by requiring the handling of large volumes of paper, a task that election officials hope to reduce or eliminate through the use of electronic voting. On the other hand, a long-term analysis might show that they can lower costs by reducing the expenses entailed in contested elections.
- What are the optimal forms in which a paper trail should be presented to the voter? Some approaches allow the voter to actually receive the paper version of their ballot in their hands, after which the voter verifies and deposits the paper version in a ballot box. Other approaches do not allow the voter to touch the paper version of the ballot at all; rather the paper ballot typically scrolls under a pane of glass, and once verified by the voter, moves to a position where it cannot be further viewed. What are the usability, reliability, security, and privacy implications of these approaches?
- To what extent are VVPATs easily accessible to voters with vision impairments? How difficult or expensive would it be to produce VVPATs for languages other than English? How can new technologies help to address problems, if any, in these areas?
- To what extent and in what ways, if any, do VVPATs affect the voter's confidence in the casting of a vote? Because a voter's actual behavior in the voting booth is private, it may be difficult to know how a voter actually uses the voter verification feature, and what impact it has on his or her confidence in the election. The feature might provide reassurance that an auditable record of his or her ballot has been generated (as advocates of the VVPAT claim), or it might introduce a measure of doubt where none existed without the feature (as some vendors claim).

6-29. **What special data collection requirements are associated with auditing elections conducted with electronic voting systems?** More generally, how should election reporting systems in toto be designed to enable good postelection analyses that check for anomalies? Election reporting systems generate data that cover all aspects of the election—including votes cast in venues other than polling places on Election Day.

6-30. **What are the costs and benefits of open standards that could facilitate the design of interoperable components for electronic voting systems?** What would these standards cover? If they are desirable, what are the impediments to developing them? Who would develop them? How should they be developed in order to avoid advantaging one vendor or another? In general, modularity and conformance to standards (e.g., data exchange standards, public applications programming interfaces) allow a marketplace to develop that is friendly to smaller companies, thus facilitating multiple alternatives in the marketplace. While this fact arguably works against the interest of a vendor that already has a significant presence in the market, it also gives potential purchasers confidence that they will not be left overly dependent on a specific vendor, and thus reduces the risk of making a commitment to an electronic voting path.

From a technical standpoint, modularity is valuable if the interface specifications between modules are clear, are well chosen, and are followed. For example, modular construction potentially enables certification of a system component by component, which means that changes in one module do not affect the behavior of other modules, and therefore an entire system can be regarded as certified if each of its constituent components is certified. On the other hand, it can be very difficult indeed to develop interface specifications that guarantee that a module interacts with the outside world only through its interfaces, and of course it is impossible to guarantee entirely modular interactions before there is agreement on the interface specifications. Moreover, assurances of a system's security are often based on the assessment of the system as a whole, and moving components in and out is likely to introduce security vulnerabilities, especially in the absence of good interface standards. It may turn out that in the long run, the benefits of a more open market facilitated by enhanced modularity outweigh the formal assurances of certifying systems as a whole. But that analysis has yet to be performed.

6-31. **What are the implications, for security and otherwise, of using multipurpose hardware for voting purposes?** Almost all of today's electronic voting systems are based on dedicated hardware and software, and so these systems are entirely useless for other purposes. Nontrivial cost savings might flow from the ability to use multipurpose equipment already owned by the jurisdiction in question for voting purposes. The

conventional wisdom is that the use of such off-the-shelf commodity equipment is not well adapted to the security and usability requirements of voting, which is a very specialized application. And this point of view may well be correct. Nevertheless, the question deserves investigation, as it may be possible to develop architectures that are more secure than the models considered in the conventional wisdom.

6-32. **What would be the desirability and content of a model election code to govern elections undertaken with electronic voting systems?** As noted in Chapter 1, the laws governing elections vary significantly by state. To ease the design burden on vendors currently in or seeking to enter the electronic voting market, it might be desirable to provide some uniformity in the requirements governing these systems. A model election code might be established, in spirit patterned after projects initiated by the National Commissioners of Uniform State Laws (NCUSL). The NCUSL have worked effectively with states to establish—among other uniform state laws—the Uniform Commercial Code. Such uniformity would promulgate a framework with which vendors could more easily work.

To illustrate an issue that may become relevant in the future, consider the question of what is regarded as the official record of an election. The proposed technical guidelines for voting system security include the requirement for independent dual verification (IDV) of the voter's ballot. IDV is the idea that the voter's casting of a ballot results in two records of that vote, separately maintained and stored. But when two records are generated of a single transaction, what is to be done if and when there is a discrepancy between them? Which one is the record that will be used in recounts, for example?

6-33. **How and to what extent have notions of voter privacy and secrecy changed over time and with the introduction of new voting technologies?** Many concepts change along with changes in the cultural and social milieu in which those concepts are embedded, so one can easily imagine that notions of voter privacy and secrecy might have done so as well. Some analysts argue, for example, that there has been an accumulating erosion of voting privacy over the last decade, and that virtually every technical improvement or change in the election law in recent years has been at the expense of voter secrecy rights. Others suggest that there are potential conflicts between some dimensions of an election system's transparency and voter privacy. An explicit understanding of these issues might help to frame discussion of further changes in election law, policy, or technology.

6-34. **How and to what extent is secure absentee voter registration feasible?** For individuals who are living in locations other than the precincts where they are or should be registered to vote (e.g., individuals on

military deployments or working abroad), absentee voter registration would greatly facilitate their ability to participate in local elections. On the other hand, absentee voter registration requires methods for authenticating potential registrants that do not involve face-to-face interaction with local election officials. Absentee voter registration using electronic systems further raises the possibility that falsified voter registration might be undertaken on a large scale.

The committee also wishes to call attention to a research agenda for electronic voting developed at a workshop of the American Association for the Advancement of Science (Box 6.3).

Box 6.3
The AAAS Research Agenda for Electronic Voting
(Selected Excerpts)

To maximize the value of any research conducted, workshop participants [at the AAAS Workshop on Electronic Voting, held September 17-18, 2004] acknowledged the importance of achieving a common understanding across research fields of key concepts on which further study should focus and of identifying useful data and research methods. They recommended a set of 13 key concepts that warrant clearer definitions and more precise methods for measuring them and assessing their impact on the voting system:

- *Accessibility* and *equal protection* regarding all components of the voting system;
- *Accuracy* as it applies to recording and counting votes;
- *Anonymity* and *privacy* as they relate to the casting of a vote, as well as to efforts undertaken to ensure accountability in voting systems;
- *Error* and *fraud* with regard to their occurrence throughout the system;
- *Intent* with respect to determining whether voting technologies capture the vote as it was intended;
- *Transparency* in terms of maximizing accountability while preserving legitimate privacy rights;
- *Vulnerability, threat*, and *risk* so that comparative assessments can be made of alternative voting technologies and other proposed changes to the voting system; and
- *Usability* to evaluate how any technology can be assessed for ease of use by voters or other actors in the system.

Research on Voting Technologies

Several research questions were identified related to the design, adoption, use, evaluation, and certification of alternative voting technologies, [including vot-

(continued)

Box 6.3 continued

ing machines,] databases used for voter registration, the ballots used on Election Day, and the techniques used to test and evaluate the performance of the voting machines.

- What does it mean for a voting technology to perform "up to standard"? What are the proper metrics to use for measuring performance? What should be included in a standards-setting process for voting technologies? What are the best ways for developing and monitoring standards, and how should various stakeholders be involved? How can voting technologies best be tested in the field for meeting performance standards?. . .

Research on Voter Knowledge, Perception, and Behavior

Research should be aimed at discovering ways in which the voting system does or does not serve the needs of the voter.

- What factors discourage or encourage citizens to engage the voting system? What impact is the provisional ballot having on voter participation?
- When voter turnout in a specific jurisdiction is underestimated, how does it affect voter access to the polls? How are lines of voters managed, and how long a wait are people willing to tolerate in order to vote?
- From where do voters acquire information about the voting system? What are the strengths and weaknesses of alternative strategies for disseminating voting information?. . .

Research on Election Administration

One of the more overlooked components of the voting system by researchers has been how the voting process is administered. . . . Workshop participants [at the September 2004 AAAS workshop on electronic voting] noted the increasing responsibilities that the voting system places on election officials. Questions surrounding their role, preparation, and resources received considerable attention.

- What is the level of professionalism among election officials? How do differences in skill sets affect their performance, and with what impact?
- What efforts are taken by election officials to help voters navigate the voting system?
- Who makes decisions about which voting technologies to adopt, and what factors are considered? What is the nature of the relationship between technology vendors and election officials? Is there oversight of the relationship; if so, by whom?

Research on Accountability Mechanisms

Holding people and technology accountable is critical to conducting and certifying elections and to generating public confidence in the system. Workshop participants identified several research issues associated with investigating the impact and effectiveness of various accountability mechanisms.

Box 6.3 continued

- How can voters be assured that their votes were cast and counted as intended?
- What are the "best practices" for auditing elections, and who should be involved?
- What are the means by which voting technologies can be designed to provide effective audit trails (e.g., paper or computer images)? How can they be tested and validated?. . .

Research on Alternative Future Voting Scenarios

Participants noted a number of future voting scenarios that warrant careful assessment. . . . Research on how innovation of new voting technologies is affected by and affects the existing voting system is needed if we are to be better positioned to shape our "alternative future.". . .

- What impact would [distributed voting] have on voter participation, especially those subpopulations with minimal access to or experience with the types of technologies that could be used?
- What security and privacy issues are raised by such a distributed voting system?

SOURCE: Excerpted with permission from Mark S. Frankel, Tova Jacobovits, and Adrianne Kroepsch, American Association for the Advancement of Science, October 2004, available at http://www.aaas.org/spp/sfrl/evoting/report2.pdf.

7

Findings and Conclusions

In articulating the questions presented in Chapters 4, 5, and 6, the committee developed a number of findings that it believes can help to clarify the nature of the debate over electronic voting systems and provide a framework for putting these questions into perspective.

The committee believes that **electronic voting systems offer potential for voting and election management that is an improvement over what has thus far been available. However, the realization of this potential requires a commitment to this path by the nation, the states, and local jurisdictions that is not yet evident.** From facilitating or enabling alternative forms of voting (e.g., absentee voting, early voting) to increasing the comprehensibility of ballots and reducing opportunities for fraud and enhancing the accuracy of vote counts, electronic voting systems of all kinds offer possibilities for greater enfranchisement of the population at large. Because electronic voting systems cannot simply replace the voting systems already deployed and in use, a commitment to this path will require innovative and dynamic methods to develop, implement, and improve comprehensive electronic voting solutions rather than just individual components.

Further, this commitment must be understood as an ongoing effort that includes support for a new national research process, with research laboratories at the national, regional, or state levels; the implementation of research and development efforts to resolve the security and usability issues associated with existing and new election technologies; a lasting commitment to open and dynamic standards, testing, and certification

efforts for election technologies; and ongoing efforts to educate election officials, poll workers, voters, and the general public about these new election technologies.

Also, it must be recognized that the deployments of electronic voting systems in the past few years are likely to be just the beginning of a long period of adaptation to electronic technologies in election administration and management. (As one point of comparison, consider that it took about 40 years for secret ballots to be adopted nationwide.)

A second important point, obvious yet often overlooked in the public debate, is that the introduction of electronic voting systems is intended to make elections better. That is, **the desirability of electronic voting systems should be judged on the basis of whether their use will significantly improve the process of election administration.** When new voting systems offer an opportunity to significantly improve at reasonable cost the process of election administration in multiple dimensions over what it is today—for example, to make election administration more efficient, less costly, more usable and accurate, more trustworthy and secure, and so on—it makes sense to consider their deployment. On the other hand, merely marginal improvements are rarely if ever worth the cost of the disruption associated with the introduction of new systems. In general, it is reasonable to make judgments about cost-effectiveness—whether certain improvements are worth the cost of obtaining them—as long as these judgments are explicit. (In this regard, the law of diminishing returns clearly applies: the cost of the last few improvements is likely to be many times the cost of the first few.)

Moreover, **judgments about the ultimate desirability and feasibility of electronic voting systems should not be limited to the features and flaws of the systems demonstrated to date.** Today's debate over electronic voting systems has been framed largely by examination of electronic voting products available today. Irrespective of the merits of these examinations, the history of most technology-based artifacts is that early versions reflect limited operational experience and that later versions improve over time as user needs and threats to system integrity are understood better and as the underlying technology improves. It is thus inappropriate to make strong generalizations about the systems of tomorrow based solely on inspection of the systems of today.

A corollary of this finding is that because electronic voting systems are so flexible, the range of possible performance and functionality is exceedingly large. At one end, it is entirely possible to design systems that perform more poorly and are less usable and less secure than any system in use today. At the other end, there is no a priori reason that systems could not be designed to be much better with respect to nearly any set of features or requirements. What matters operationally, of course, is where

any given system offered for sale lies on this continuum, not generalizations at either end of the range.

At the same time, there are some technical realities that are exceedingly likely to persist over the long run. For instance, small software changes might (or might not) result in substantial changes to the system's behavior, and testing alone cannot prove the absence of problems. Conclusions based on such realities have a staying power that conclusions based on today's state of technology do not.

The committee also believes that **trusted election processes should be regarded as the gold standard of election administration,** where a trusted election process is one that works, can be shown to have worked after the election has been held, can be shown to have not been manipulated and to have not led to a large number of mistaken or lost votes, and can be shown to reflect the intent of the voters. As discussed in Section 2.2, trusted election processes increase the likelihood that elections will be regarded as fair, even by the losing side and even in a partisan political environment.

As for the often rancorous debate about electronic voting, the committee believes that many parties have made important contributions:

- **Electronic voting skeptics have raised important questions about the security of electronic voting systems that should not be discouraged or suppressed.** Experience indicates that the public airing of issues related to security often results in revelations of flaws that might not have been forthcoming in the absence of such airing, and the history of the electronic voting systems debate in the last few years is no exception to this experience. Skeptics have also raised the point that electronic voting systems, like all complex systems, are fallible and susceptible to deliberate or accidental compromise. Thus, it seems to the committee to be a matter of common sense that some kind of backup against the possibility of fraud or malfunction should be available if and when allegations of such occurrences arise. The paper trail may be a mechanism that can serve this function, but whether it is the only or most appropriate such mechanism has yet to be determined.
- **Political scientists who have studied elections for many years have identified data whose collection would enable the public to judge the accuracy and usability of voting systems in use and the accuracy and reliability of the voter registration systems used by states, counties, and municipalities.** Again, it seems to be a matter of common sense that independent observers need relevant and reliable data in order to judge the adequacy of the systems in use, and election officials should be encouraged to acquire such data and to make it publicly available.

• **Legislators in many states have publicly aired many important issues related to electronic voting.** In so doing, they have placed a considerable amount of useful information on the public record, and they have successfully balanced a variety of concerns in some of their legislative efforts.

At the same time, it is appropriate and proper that election officials are properly concerned about many aspects of election administration, and they must balance a variety of considerations—including security, speed and accuracy of reporting election results, usability, affordability, voter turnout, and compliance with federal, state, and local election laws. It is entirely reasonable and understandable that they take an operational perspective, as might be expressed in the question, Will a particular electronic voting system help to significantly improve election administration and management with respect to all of these considerations? If they can in good conscience answer this question in the affirmative, acquisition of such a system is justifiable.

As for the security debate per se, election officials sometimes complain that security advocates are undermining public confidence when they assert that security is an issue. But the committee believes that by responding affirmatively and openly to revelations, public officials can make improvements and also promote the public confidence that will be necessary for the widespread adoption of electronic voting. At the same time, those who advocate single-mindedly for security without explicitly acknowledging the broader concerns of election officials are inviting those officials to give their advice less consideration than might otherwise be warranted. Framing concerns about security in the larger context of all of the issues of concern will also help to improve the tone of the debate.

In developing this report, the committee took note of the significant emotion and passion felt by all participants in the public debate about electronic voting. Although such passion and emotion are often regarded as impediments to a reasoned and thoughtful public debate, the committee believes that these passions reflect—at heart—a very emotional and visceral-level commitment to the notion of democracy. One can—and people do—take issue with various arguments about technology or organization, but on balance, the committee believes that the nation is much better served by passionate engagement than by dispassionate apathy, and so the passions expressed by the various participants on all sides of the debate are to be commended rather than disparaged. The committee further hopes that the questions that it has articulated in this report can help the nation overcome political and technological barriers that may impede the improvement of the election systems in the future.

Appendixes

A

Glossary

Algorithm—a precise set of steps that can be used to solve some problem.

Audit—in an election context, an activity that seeks to validate and verify as many aspects of the election cycle as possible without violating state privacy laws. An audit may involve a recount of the votes, but this is only one of the actions that an audit may entail.

Ballot definition—the process through which a physical ballot form is created, including the selection of the contests in question and how they appear on the form.

Ballot provisioning—the process of providing a voter with the correct ballot form on which to vote.

Certification—a process undertaken by states to certify that a given voting system is acceptable for use. In principle, only certified systems may be used in an election, although the reality is sometimes at variance with this requirement.

Overvoting—an indication on a cast ballot that more than one choice has been made in a single-choice contest. Overvotes are invalid votes.

Provisional vote—a ballot cast by a voter whose credentials for voting in a particular precinct cannot be verified on Election Day. If his or her credentials are subsequently verified after Election Day, the ballot is eligible to be counted.

Qualification—a process undertaken under the authority of the federal Election Assistance Commission to "qualify" voting systems. An independent testing authority, designated by the National Association of State Election Directors (NASED), evaluates a voting system to see

if it meets or exceeds the Federal Elections Commission's 2002 Voting Systems Standards.

Residual vote—the sum of overvotes and undervotes for a given election contest.

Source code—a computer program rendered in human-readable form that also clearly lays out the structure of the program.

Undervoting—a lack of indication on a cast ballot about the voter's choice for a given contest. Undervotes are legal, because there is no requirement that a voter must vote on every contest, but may or may not reflect the actual intention of the voter in casting (or not casting) a vote for the contest in question.

Voter-verified paper audit trail—a physical paper record of voter ballots as voters have cast them on an electronic voting system that the voter may verify corresponds to his or her intent in casting those votes.

Voting station—the physical unit on which a voter casts a vote. Any given electronic voting system may involve hundreds of identical voting stations located in many different precincts.

B

Committee and Staff Biographies

COMMITTEE MEMBERS

Dick Thornburgh, *Co-chair*, served as governor of Pennsylvania, attorney general of the United States, and under-secretary-general of the United Nations during a public career that spanned more than 25 years. He is currently counsel to the international law firm of Kirkpatrick & Lockhart Nicholson Graham, LLP, resident in its Washington, D.C. office. Elected governor of Pennsylvania in 1978 and reelected in 1982, Governor Thornburgh was the first Republican ever to serve two successive terms in that office and was named by his fellow governors as one of the nation's most effective big-state governors in a 1986 Newsweek poll. After his unanimous confirmation by the U.S. Senate, Governor Thornburgh served 3 years as attorney general of the United States (1988-1991) under Presidents Ronald Reagan and George H.W. Bush. He was educated at Yale University, where he obtained an engineering degree, and at the University of Pittsburgh School of Law, where he served as an editor of the Law Review. Governor Thornburgh served as director of the Institute of Politics at Harvard's John F. Kennedy School of Government (1987-1988). He is a member of the board of directors of the University of Pittsburgh, the Urban Institute, and the Gettysburg National Battlefield Museum Foundation. The governor was the founding chairman of the State Science and Technology Institute and is vice-chairman of the World Committee on Disability. He was selected as a lifetime national associate of the National Academies in 2001 and chaired the National Research Council studies

Harnessing Science and Technology for America's Economic Growth (1999) and *Youth, Pornography, and the Internet* (2002).

Richard Celeste, *Co-chair*, is a native of Cleveland, Ohio. After graduating magna cum laude and Phi Beta Kappa from Yale University in 1959, he attended Oxford University in England as a Rhodes scholar. After a short term as a staff liaison officer in the Peace Corps, Ambassador Celeste worked for 4 years as special assistant to the U.S. ambassador to India in New Delhi. Following this, Ambassador Celeste returned to his native Ohio, where he served as a state representative for 4 years and lieutenant governor for a further 4 years. After an unsuccessful campaign for governor, he was asked by President Carter to serve as director of the Peace Corps. After 2 years, Ambassador Celeste returned to Ohio to wage a successful quest for the governor's office. Celeste was elected in 1982 and reelected in 1986. Barred by Ohio's constitution from seeking a third term, Ambassador Celeste became a managing partner in the business consultancy Celeste & Sabety Ltd., in Columbus, Ohio. On November 10, 1997, Richard Celeste was sworn in as the U.S. ambassador to India, a post he held until April 2001. In July 2002, Celeste was inaugurated as the 12th president of Colorado College, a highly selective liberal arts college founded in 1874. Ambassador Celeste serves as chairman of the Health Effects Institute in Boston. He is a member of the Council on Foreign Relations.

R. Michael Alvarez is professor of political science at the California Institute of Technology. He received a B.A. from Carleton College in 1986 and a Ph.D. from Duke University in 1992. At Caltech, his research has focused on elections, voting behavior, and survey and statistical research. Since 2000, much of his work has centered on the Caltech/MIT Voting Technology Project, which he currently codirects. As part of his efforts to study the electoral process, Dr. Alvarez has published a number of studies. He wrote (with Thad E. Hall) *Point, Click, and Vote*, published in early 2004, his third book. He is now writing another book with Hall on the electronic voting controversy. The recipient of many grants and awards, Dr. Alvarez was named to the *Scientific American* 50 in 2004 for his efforts in the field of voting technologies and electoral processes.

Thomas Sheridan is Ford professor emeritus of engineering and applied psychology in the Departments of Mechanical Engineering and Aeronautics and Astronautics at Massachusetts Institute of Technology (MIT) and director of the Human-Machine Systems Laboratory there. His research has been on mathematical models of human operator and socioeconomic systems, on man-computer interaction in piloting aircraft and in super-

vising undersea and industrial robotic systems, on computer graphics technology for information searching and group decision making, and on arms control. Dr. Sheridan has an S.M. degree from the University of California, an Sc.D. from MIT, and an honorary doctorate from Delft University of Technology, the Netherlands. He served as president of both the Human Factors and Ergonomics Society and the IEEE Systems, Man and Cybernetics Society and is a fellow of both organizations. Dr. Sheridan chaired the National Research Council's Committee on Human Factors and has served on numerous other NRC committees. He is senior editor of the journal *Presence: Teleoperators and Virtual Environments* and is a member of the National Academy of Engineering.

Joseph Smialowski was named Freddie Mac's executive vice president of Operations and Technology in December 2004. Prior to joining Freddie Mac, Mr. Smialowski was executive vice president at Fleet Boston Financial, where he was part of the firm's management committee and had direct oversight of information technology, bank operations, corporate real estate, procurement, security and business continuity for Fleet's business lines in Asia, Europe, Latin America, and the United States. Mr. Smialowski held a key position on the integration team following the acquisition of Fleet Boston by Bank of America. Prior to joining Fleet Boston in 1998, he was chief information officer at Sears, Roebuck and Co., overseeing all of the information technology units for the company's retail, credit, product service and direct-response businesses in North America. During this time, Mr. Smialowski also served as chairman of the National Retail Federation's Technology Council and was a recipient of the National Center for Supercomputing's Grand Challenge Award. He received a B.A. in philosophy from Merrimack College and a master's degree in computer systems management from the Rochester Institute of Technology.

Anthony Stevens is assistant secretary of state for New Hampshire, a position he has held since 1994. In this role, he has served as the New Hampshire coordinator for the Help America Vote Act, serves as project manager for the statewide voter registration system, and is part of the management team engaged in purchasing voting systems equipped for accessibility. Prior to taking his current position, he was vice president for corporate lending at Citicorp/Citibank and a member of the New Hampshire State Legislature for two terms. He received an M.B.A. from the Harvard Business School and an undergraduate degree in economics, summa cum laude, from the University of New Hampshire. He is a current member of the National Association of State Election Directors.

Peter Weinberger has a Ph.D. in mathematics (number theory) from the University of California at Berkeley. After teaching mathematics at the University of Michigan in Ann Arbor, he moved to Bell Laboratories. At Bell Labs he worked on Unix and did research on topics including operating systems, compilers, network file systems, and security. Dr. Weinberger then moved into research management, ending up as Information Sciences Research vice president, responsible for computer science research, math and statistics, and speech. His organization undertook productive new initiatives, one using all available call detail to detect fraud and another doing applied software engineering research to support building software for the main electronic switching systems for central offices. After Lucent and AT&T split, Dr. Weinberger moved to Renaissance Technologies, a technical trading hedge fund, as head of technology, responsible for computing and security. In 2003 he moved to Google in New York, where he is now.

STAFF MEMBERS

Herbert S. Lin is senior scientist and senior staff officer at the Computer Science and Telecommunications Board, National Research Council of the National Academies, where he has been study director of major projects on public policy and information technology. These studies include a 1996 study on national cryptography policy (*Cryptography's Role in Securing the Information Society*); a 1991 study on the future of computer science (*Computing the Future*); a 1999 study of Defense Department systems for command, control, communications, computing, and intelligence (*Realizing the Potential of C4I: Fundamental Challenges*), and a 2000 study on workforce issues in high-technology (*Building a Workforce for the Information Economy*). Prior to his NRC service, Dr. Lin was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He also has significant expertise in math and science education. He received his Ph.D. in physics from MIT in 1979. Avocationally, he is a long time folk and swing dancer, and a poor magician. Apart from his CSTB work, a list of publications in cognitive science, science education, biophysics, and arms control and defense policy is available on request.

Kristen Batch is a research associate with the Computer Science and Telecommunications Board of the National Research Council. She will be involved with upcoming projects focusing on wireless communication technologies and telecommunications research and development. While pursuing an M.A. in international communications from American University, she interned in the Office of International Affairs at the National

Telecommunications and Information Administration, and in the Technology and Public Policy Program at the Center for Strategic and International Studies. Ms. Batch also earned a B.A. from Carnegie Mellon University in literary and cultural studies and Spanish and received two travel grants to conduct independent research in Spain.

Ted Schmitt is a consultant for the Computer Science and Telecommunications Board of the National Academies. Schmitt is currently involved in the CSTB projects providing a comprehensive exploration of cybersecurity and the use of IT to enhance disaster management. Before CSTB, Ted was involved in the development of the digital publishing industry and has taken an active role in various standards groups related to digital rights management. Prior to that, he served as technical director at a number of small technology companies in Germany, Sweden and the United States. He started his career in 1984 as a software engineer for IBM, earning two patents. Ted is currently working on his M.A. in international science and technology policy at George Washington University. His graduate work is supported by a fellowship from the Diplomat and Consular Officers – Retired. He received a B.S. in electrical engineering in 1984 and a B.A. in German in 1997 from Purdue University and studied at the University of Hamburg, Germany.

C

Contributors to the Study

PARTICIPANTS IN THE JULY 2004 NRC WORKSHOP ON ELECTRONIC VOTING

Dick Thornburgh (workshop chair)
R. Michael Alvarez, California Institute of Technology
Faye Anderson, Consultant
Stephen Ansolabehere, Massachusetts Institute of Technology
Henry Brady, University of California, Berkeley
Doug Chapin, Electionline.org
David Chaum, DigiCash Inc.
Kevin Chung, AVANTE International Technology, Inc.
Dana DeBeauvoir, Travis County, Texas
Jim Dickson, American Association of People with Disabilities
David L. Dill, Stanford University
Eric Fischer, Congressional Research Service
Susan Inman, Little Rock, Arkansas
Wendy Kellogg, IBM
Linda Lamone, State of Maryland
Martha Mahoney, University of Miami School of Law
Gary McIntosh, McIntosh Election Services
Sanford Morganstein, Populex Corporation
Ian Piper, Diebold, Inc.
Sharon Priest, The Downtown Partnership

Ronald Rivest, Massachusetts Institute of Technology
Scott Robertson, Drexel University
Aviel Rubin, Johns Hopkins University
Ted Selker, Massachusetts Institute of Technology
Michael Shamos, Carnegie Mellon University
Thomas Sheridan, Massachusetts Institute of Technology
Joseph Smialowski, Fleet Boston Financial
Peter Weinberger, Google Inc.
John T. Willis, Bowie and Jensen

BRIEFERS AND PRESENTERS TO THE COMMITTEE, DECEMBER 9, 2004

Jim Adler, VoteHere, Inc.
Kim Alexander, California Voter Foundation
Tom Auriemma, New Jersey State Division of Gaming Enforcement
Ren Bucholz, Electronic Frontier Foundation
Drew Dean, SRI
Herb Deutsch, IEEE Committee on Voting Equipment Standards
Rick Hasen, Loyola Law School
David Jefferson, Lawrence Livermore National Laboratory
Douglas Jones, University of Iowa
Linda Lamone, Maryland State Board of Elections
Eric Lazarus, DecisionSmith
Linda Lindberg, General Registrar, Arlington County
Rebecca Mercuri, Association for Computing Machinery
Peter Neumann, SRI
Scott Scherer, Nevada Gaming Control Board
Nancy Tate, League of Women Voters
Dan Tokaji, Ohio State University
Rebecca Vigil-Giron, New Mexico Secretary of State, National Association of Secretaries of State
David Wagner, University of California, Berkeley

BRIEFERS AND PRESENTERS TO THE COMMITTEE, APRIL 22, 2005

Neil McClure, Hart InterCivic
Ron Rivest, Massachusetts Institute of Technology

LIST OF WHITE PAPERS RECEIVED BY THE COMMITTEE[1]

The Need for Transparent, Accountable, and Verifiable U.S. Elections, Kim Alexander, California Voter Foundation

Privacy Issues in an Electronic Voting Machine, Arthur Keller, David Mertz, Joseph Lorenzo Hall, and Arnold Urken

A PC-Based Open-Source Voting Machine with an Accessible Voter-Verifiable Paper Ballot, Arthur Keller et al., Open Voting Consortium

Preliminary Analysis of E-Voting Problems Highlights Need for Heightened Standards and Testing, Deirdre Mulligan and Joseph Lorenzo Hall, University of California, Berkeley

Electronic Voting Machines and the Standards-Setting Process, Eddan Katz and Rebecca Bolin, Yale University School of Law

Illustrative Risks to the Public in the Use of Computer Systems and Related Technology, Excerpt: Election Problem Cases as of Novermber 25, 2004, Peter G. Neumann, SRI International

Putting People First: The Importance of User-Centered Design and Universal Usability to Voting Systems, Sharon Laskowski, National Institute of Standards and Technology, and Whitney Quesenbery, Whitney Interactive Design LLC

Accessibility and Auditability in Electronic Voting, Electronic Frontier Foundation

Electronic Voting, David Dill and Will Doherty, Verified Voting Foundation

Electronic Voting Machines in South Carolina, Duncan Buell and Carter Bays, University of South Carolina

The Need for Usability of Electronic Voting Systems: Questions for Voters and Policy Makers, ACM Special Interest Group on Computer-Human Interaction (SIGCHI), U.S. Public Policy Committee

Voting, Vote Capture and Vote Counting Symposium: Electronic Voting Best Practices, Jean Camp, Allan Friedman, and Warigia Bowman, Harvard University, John F. Kennedy School of Government

Making Each Vote Count: A Research Agenda for Electronic Voting, report of a AAAS workshop on electronic voting, October 2004

Electronic Voting Systems: The Good, the Bad, and the Stupid, Barbara Simons

[1]These papers are available in their entirety at http://www7.nationalacademies.org/cstb/project_ evoting.html#papers.

What Is CSTB?

As a part of the National Research Council, the Computer Science and Telecommunications Board (CSTB) was established in 1986 to provide independent advice to the federal government on technical and public policy issues relating to computing and communications. Composed of leaders from industry and academia, CSTB conducts studies of critical national issues and makes recommendations to government, industry, and academic researchers. CSTB also provides a neutral meeting ground for consideration of complex issues where resolution and action may be premature. It convenes invitational discussions that bring together principals from the public and private sectors, ensuring consideration of all perspectives. The majority of CSTB's work is requested by federal agencies and Congress, consistent with its National Academies context.

A pioneer in framing and analyzing Internet policy issues, CSTB is unique in its comprehensive scope and effective, interdisciplinary appraisal of technical, economic, social, and policy issues. From its early work in computer and communications security, cyber-assurance and information systems trustworthiness have been cross-cutting themes in CSTB's work. CSTB has produced several reports regarded as classics in the field, and it continues to address these topics as they grow in importance.

To do its work, CSTB draws on some of the best minds in the country, inviting experts to participate in its projects as a public service. Studies are conducted by balanced committees without direct

financial interests in the topics they are addressing. Those committees meet, confer electronically, and build analyses through their deliberations. Additional expertise from around the country is tapped in a rigorous process of review and critique, further enhancing the quality of CSTB reports. By engaging groups of principals, CSTB obtains the facts and insights critical to assessing key issues.

The mission of CSTB is to

- *Respond to requests* from the government, nonprofit organizations, and private industry for advice on computer and telecommunications issues and from the government for advice on computer and telecommunications systems planning, utilization, and modernization;
- *Monitor and promote the health* of the fields of computer science and telecommunications, with attention to issues of human resources, information infrastructure, and societal impacts;
- *Initiate and conduct studies* involving computer science, computer technology, and telecommunications as critical resources; and
- *Foster interaction* among the disciplines underlying computing and telecommunications technologies and other fields, at large and within the National Academies.

More information about CSTB can be obtained online at http://www. cstb.org.