MAKING EVERY VOTE COUNT:

SECURITY AND RELIABILITY OF COMPUTERIZED VOTE-COUNTING SYSTEMS

Lance J. Hoffman

Original report published internally and distributed to workshop participants by The George Washington University Institute for Information Science and Technology, Report IIST-87-17, Department of Electrical Engineering and Computer Science, School of Engineering and Applied Science, Washington, DC, December 1987.

MAKING EVERY VOTE COUNT:

SECURITY AND RELIABILITY OF COMPUTERIZED VOTE-COUNTING SYSTEMS

Lance J. Hoffman

School of Engineering and Applied Science
Department of Electrical Engineering and Computer Science
The George Washington University
Washington, D. C. 20052

2nd Printing, March 1988

MAKING EVERY VOTE COUNT:

Preface

This report examines the security, accuracy, and reliability of vote-counting systems. Problems with security and accuracy also arise in other parts of the election process (in registration and polling place practices, for example). These, however, are beyond the scope of this report, except as they relate to vote counting. Other issues, such as the effects of voting systems on voter participation, are also beyond the scope of this report.

In writing this report, I have drawn upon previously published literature; discussions with federal, state, and local election officials; meetings with vendors and computer security specialists; and vendor literature and documentation. The report's conclusions are derived from a three-day invitational workshop in which 26 election officials, computer scientists, vendors, and other election experts participated. However, the report does not necessarily reflect the position of the workshop sponsor, participants, or their employers. Indeed, every workshop participant probably would not agree with every sentence. I have tried to be faithful to what I heard, but I am solely responsible for the opinions expressed here.

From a background in computer security, I have attempted to listen carefully to two "cultures"--the computer science community and the election administration community. Both agree that the vast majority of the problems are administrative. The recommendations made in this report, therefore, are largely organizational, not technical. They will be useful to county and state election officials, state legislators, the Federal Election Commission, vendors of election equipment, Congress, and all others who are concerned about the integrity of elections in the computer age.

I have had a great deal of help from a number of people through this entire project:

o My informal advisory committee: Richard Smolka, of Election Administration Reports; Marie Garber, then administrator of the State Administrative Board of Election Laws for Maryland; Willis H. Ware, a security expert and senior scientist at the Rand Corporation; and Robert J. Naegele, an independent consultant and president of Granite Creek Technology, Inc. They candidly gave me valuable advice on structuring the workshop on which most of this report is based.

o Fred Weingarten, of the U.S. Office of Technology Assessment; Emmett Fremaux, Jr., executive director of the District of Columbia Board of Elections and Ethics; and

Robert Tyre, formerly with Arthur Young & Company, who led the small discussion groups at the workshop.

o Penelope Bonsall, director of the National Clearinghouse on Election Administration of the Federal Election Commission, and Kim Brace, president of Election Data Services, Inc. They unselfishly gave their time and resources to a computer scientist who had somehow strayed into the elections field.

o Roy Saltman of the National Bureau of Standards, who shared his considerable knowledge of the technological difficulties in "problem elections."

o Louisa Hogan, my former aide at The George Washington University, who put up with misplaced agendas and an absent-minded professor and who assisted ably at the workshop with diplomacy and panache.

o Joe Younger, whose editing has made this report much more readable and understandable than its first draft.

o Paula Newberg of the Markle Foundation, who insisted that the work be good, rather than on time.

o And, most important, Larry Slesinger of the Markle Foundation, without whose insight, support, knowledge, enthusiasm, prodding, and common sense neither the workshop nor the report would have ever seen the light of day.

There are a great many other people who were very helpful, especially in answering questions about specific topics. You know who you are, and I thank you.

TABLE OF CONTENTS

1. Introduction

Democracy depends on people trusting both their elected officials and the process that puts those officials in office. That process includes elections. In the United States, elections are held in thousands of jurisdictions every year. Each voter in those jurisdictions deserves to have his or her vote accurately counted. Indeed, such accuracy is essential to representative democracy.

U.S. elections now depend heavily on computers. Computers are important in organizing direct mail fund-raising campaigns, dissecting the electorate demographically, and analyzing voting records and past statements on issues. In recent years, journalists, academic researchers, political consultants, and politicians have debated and analyzed these uses of the computer. Less attention, however, has been paid to a more fundamental use of computers in elections: how they record and tabulate votes.

Today, most voters cast their ballots on systems that use a computer to record or tabulate votes. In much of the United States, people vote by marking a punch card or sheet of paper that is then fed into a computer system for tabulation; in some cases, all-electronic voting machines (analogous to mechanical lever machines) are used; some of these produce no paper record of the vote cast. In the 1984 election, only three out of ten jurisdictions in the United States still used paper ballots, and these accounted for only about 10 percent of the total votes cast.[1]

Despite the public attention and sometimes high emotions accompanying elections, most jurisdictions in the United States quietly count their votes, apparently correctly. Computers have improved election administration in many ways; elections are faster and far more "voter-friendly" than ever before. And the vote-counting is probably more accurate than it was when bleary-eyed poll workers counted paper ballots into the night.

But problems do arise and can be amplified and complicated by computer systems. Some defeated candidates have filed lawsuits alleging that the system counted ballots incorrectly and caused their defeat. Although no court has yet set aside an election based on these claims, some election officials are beginning to realize that computerization cannot ensure accuracy and integrity. Some recent problem elections point out a few representative difficulties with computer-based vote-counting systems:

o In Dallas County, Texas in 1985, a recount showed significant changes in vote counts, possibly because the chad (the piece of material punched out to form a hole in a punch card ballot) was incompletely removed during the first count. In addition, precinct totals did not add up to county-wide totals.[2]

o In the 1982 election in the Third Congressional District of Indiana, an unsuccessful lawsuit claimed that the voting machine vendor representative made undocumented changes in the computer's instructions.

o In Oklahoma County, Okla., in 1986, some vote-counting machines failed to read up to 10 percent of the ballots per precinct.

o In Moline, Ill., in 1985, a faulty timing belt slipped intermittently on one card reader. This led to a miscount in which the wrong candidate actually assumed office and later had to give it up.[3]

o In San Francisco in 1983, an electrical power fluctuation added votes to one candidate's total. The startling results prompted officials to investigate the program.[4]

o Recent Illinois pre-election tests discovered errors in 28 percent of the vote-counting systems;[5] in each instance, the problem was corrected. However, Michael L. Harty, director of voting systems and standards for the Illinois State Board of Elections, testified before the Illinois Senate Republican Task Force on Vote Fraud that "the incidence of these errors in computer vote tabulation programs, as well as known tabulation errors, ... suggests ... that some vote tabulation errors go undetected."[6]

Election officials, who usually work for state and county governments and have the statutory authority and responsibility to run elections, have become increasingly concerned by accusations of improper vote counts. Often, officials have little technological expertise available when a problem occurs. Both election officials and the press often attribute difficulties to "the computer" when human beings or manual procedures are the cause. And, in relatively complex systems involving both people and machines, it's not always easy to tell where the real problem lies.

Most problems attributed to the computer system are simply human errors, not software or hardware errors. Although fraud was not involved in the cases above, the effect was the same: ballots were improperly tallied. Deterring and preventing errors and fraud in computer and manual systems depends on proper management procedures and an unalterable, properly protected "audit trail," as defined below.

2. Definitions

One problem in discussing the security and reliability of computerized vote counting is that no standardized glossary of terms exists for election administration. An election administrator may have little or no computer expertise, and a computer expert may have no knowledge of election administration beyond what he or she observes at the polling place. The definitions below will help establish some common terms.

Types of Computerized Voting Machines

In elections in which computer systems count votes, votes are typically cast one of three ways:

o An **optical scanning** voting system records marks that a voter makes (preferably with a No. 2 pencil) on one or both faces of a ballot card or series of cards. A computerized system then reads these marks to tabulate votes. Many standardized, multiple-choice tests for students (SAT or IQ tests, for example) use this type of system (also called a mark sense system) to read answers penciled on relatively stiff answer sheets.

o A **punch card** system records votes made by punches in a ballot card or series of cards.

o A **direct recording electronic** system is one in which a voter touches the ballot face with a light pen or depresses a membrane switch or button to cast a vote. Often this type of system is referred to as a direct electronic system.

Setup (Coding) for Specific Elections

Before the election, each contest must be "coded" accurately. **Coding** means assigning specific ballot positions in the computer system to the candidates or issues being voted on. For example, if certain positions on a punch card are reserved for the county clerk contest, one of these might be reserved for votes for candidate Jones, and another for votes for candidate Smith. This is typically done by setting up tables in the computer software.

Computer experts define "coding" differently. They often use **coding** as a synonym for **programming** (writing instructions in an unambiguous language that, when translated to a language the computer understands, will cause the computer to perform the desired operations). We shall not use the term in this sense here.

Coding must take into account "rotation of candidates," the requirement in some states to change the order in which candidates' names appear on the ballot. Rotation ensures that a particular candidate's name does not appear first in all ballots in all precincts.

Tests

Before any votes are cast, a number of tests should be run. There are four types of tests: qualification, certification, acceptance, and pre-election logic and accuracy.

A **qualification test** evaluates how a system complies with generic requirements (e.g., the upcoming Federal Election Commission [FEC] voluntary standards, described later in this report). A qualification test includes an examination of hardware and software, environmental hardware tests (checking whether the machines operate at certain temperatures, for instance), software ballot counting logic tests (checking whether the program counts correctly), documentation review, and other tests. To pass the qualification test, the system's generic characteristics must meet or exceed all the performance requirements. A majority of the testing done on vendor-supplied systems is qualification testing.

Certification testing ensures that the equipment complies with state law. It should include functional ballot logic tests, which reflect state law (for example, how to count ballots where a voter has cast a straight-party vote by pushing a single lever but has also voted for a candidate from another party on the same ballot). States perform certification tests after the system has passed its qualification test.

Acceptance tests confirm that the system accurately processes ballots, accepts valid votes in defined ballot positions, rejects overvotes (voting for more candidates for a particular office than allowed by law), generates status and error messages to keep the computer system operator informed during vote counting, and generates audit trails (discussed below). Local jurisdictions conduct acceptance tests after a system is purchased but before its components are contractually accepted.

Pre-election logic and accuracy tests ensure that the equipment accurately counts each specific contest in the upcoming election. Local jurisdictions carry out this type of test, also known as "the public test," before each election. After this test, the software is safeguarded so that it cannot be changed before the election.

Audit Trails

One reason computerized voting systems have sometimes been suspect is that, in general, they have not automatically maintained an unalterable "audit trail" to deter or prevent fraud. An audit trail is a record of every significant action by the computer system before, during, and after the hours the polls are open. For proper computer security, a complete audit trail must include not only a record of exceptional events, but also an electronic representation of each vote cast. Voter privacy can be ensured by either encrypting the coded "ballot images" or scrambling the order in which they are stored.

3. Relevant Findings and Recommendations from the Saltman Report

In 1974, recognizing concerns expressed by Congress, election officials, and the public, the Clearinghouse on Election Administration (then a component of the Office of Federal Elections of the General Accounting Office) requested the Institute for Computer Sciences and Technology of the National Bureau of Standards to study the use of computers in vote tallying. As expressed by Roy Saltman of the National Bureau of Standards, the concerns were (and are) that "increasing computerization of election-related functions may result in the loss of effective control over these functions by responsible authorities and that this loss of control may increase the possibility of vote fraud."[7] The institute, in a project directed by Saltman, examined election system design, training of election officials, ballot accountability, certification and inspection of computer programs, independent audits of election processes, security provisions in counting centers, and ballot recounts.

The Saltman report's findings and conclusions included the following:

o Management failures have been responsible for most of the problems with computer-based vote-counting systems. Sudden technical failures have not been a significant factor. Better management would have discovered most of the problems and prevented the related technical and human operational failures.

o Many of the difficulties in computerized elections have resulted from management's failing to appreciate the complexities of the task. A computerized election is a development project with an absolutely fixed deadline; it requires component acquisition, complete and unambiguous operational procedures, and training a large part-time staff. The project is undertaken in the expectation that the completed system will operate flawlessly the first time.

o Procedures for controlling and handling ballots, processing and reporting vote-tallying information, controlling the operation of computer programs and equipment, designing and documenting computer programs, and controlling the sites for vote tallying very often leave much to be desired. Although no one has (yet) discovered a deliberate attempt to rig a vote-counting program or proved fraudulent manipulation in court, most jurisdictions cannot demonstrate that unauthorized alterations of computer programs or other manipulations have not already taken place.

o A significant number of jurisdictions lack written specifications and acceptance testing procedures for electronic and mechanical components. Many also do not perform enough simulation, testing, and checking of the election system.

o Election administrators and vendors must agree beforehand on specific responsibilities each will assume during an election. Conflict of interest may become a serious concern if vendors assume responsibility for running any part of an election. Most jurisdictions lack the appropriate technological expertise. In those jurisdictions, vendors are likely to conduct a significant part of the election on the administration's behalf. States should ensure that each local jurisdiction possesses the necessary expertise so that it need not rely primarily on vendors of election system components.

o There is no significant funding for research and development of election equipment and no organized technical information collection and exchange program among election administrators. In general, election administrators need more training in computer security and project management. National minimum standards for accuracy and security of election procedures and equipment would be valuable.

The report made detailed recommendations (see Appendix D) that are still relevant and waiting to be implemented. Not much has changed since the Saltman report issued these findings and conclusions in the mid-1970s. As Willis H. Ware, a computer security expert from the Rand Corporation, said of the election scene in early 1987, "[The Saltman report] says it all."[8]

This report discusses developments since the Saltman report, analyzes why its recommendations have generally not been implemented, and explains how they can in fact be adopted.

4. Computer-Based Vote-Counting Problems

Widespread Use of Computers for Vote Tallying

About 54 percent of the votes cast in the United States are counted by computer, excluding aggregation of reports from mechanical lever machines. Most jurisdictions purchase or rent the computers from vote-counting machine companies, but sometimes a jurisdiction uses its own (or borrowed or rented) computers to run programs that it has designed itself, adapted from another jurisdiction, or purchased from a vendor.

Figure 1 gives a taxonomy of the major commercially available voting systems. In a survey of 31 major cities in the United States, nine still rely on lever machines. The rest have replaced these or paper ballots with computer-based vote counting systems.[9] In the period January 1986-August 1987, users of lever machines and paper ballot systems declined over 1.8 percent; these were replaced by punch card, electronic, or optical scan equipment.[10]

- Mechanical Lever
    - Sequoia Pacific
    - Shoup
- Punch Card
    - Central Count
        - Business Records Corp.
        - Sequoia Pacific
        - International Technology Group
        - Triad Governmental Systems
        - DFM, Inc.
    - Precinct Count
        - Business Records Corp.
- Optical Scan
    - Central Count
        - American Information Systems
        - Business Records Corp.
        - DFM, Inc.
        - Data Information Management Systems
    - Precinct Count
        - Business Records Corp.
        - Data Information Management Systems
- Electronic
    - Shoup
    - Sequoia Pacific
    - Business Records Corp.
    - Microvote

Figure 1. Commercially Available Voting Systems

Although vote counting seems to be a classic application of data processing--adding up the marks on ballots or holes in punch cards--problems can crop up. Typical errors occur in counting, for example, when a person votes the straight-party ticket by pressing a single lever and also votes for one member of another party, or when the law requires rotation of candidates' names on different precincts' ballots. The laws that govern counting of such complicated votes may not be implemented correctly in the programs. Both coding and programming errors have occasionally slipped in, though the former are far more prevalent.

Guarding against fraud requires good management procedures and an unalterable, properly protected audit trail. Vote-counting systems sometimes lack the first characteristic and often lack the second. In some instances, one person has been entrusted with developing and later maintaining the vote-counting program. In other cases, the vendor-supplied program may allow inclusion of user-supplied software. In either case, it is relatively easy to write a "Trojan horse" election program: one that appears to tabulate correctly but in fact secretly skews the results. For example, such a program might perform successfully during the public test but also produce results favorable to a particular candidate during the actual election.

Voting systems are vulnerable for several reasons: the inadequacy of pre-election tests, the lack of meaningful audit trails in most vote-counting programs used today, and the difficulty of ascertaining how a program truly behaves even if "source code" (the instructions, written in a computer language, that the computer translates into a program it can run) is available for inspection.

Increasing Awareness of Problems

The first alarms about the security and reliability of computer-based elections were raised at least as early as 1970.[11] In response, improvements were made in a few cases. Recently, the media have again begun to question the trustworthiness of computer-based elections. Articles have appeared in the past year or so in the computer trade press,[12] the political trade press,[13] computer bulletin boards,[14] and local and national newspapers. Legislative testimony has also focused on the problem.

In 1986, concerned activists held a grass roots convention in the Boston area. Among the speakers were Terry Elkins of Texas and Eva Waskell of Virginia, who have become alarmed at what they consider a lack of security safeguards in computerized vote-counting systems. Waskell and Elkins have also spoken around the country on the problem, often to the chagrin of election officials, and recently coauthored an article on election system security.[15] Elkins spoke before the Texas House of Representatives Elections Committee about difficulties in voting with punch card systems. In these hearings, a picture emerged of computer election systems susceptible to failure or fraud and effectively unauditable. The result was a 1987 Texas law that authorizes recertifying all vote-counting systems sold in Texas and depositing the source code and user and operator manuals with the secretary of state.

Most attempts to critically examine existing systems have been privately funded; typically, no resources have been available to screen documentation and clarifications or examine the software in detail. The quality of testimony or completeness of evidence has thus varied greatly.

5. The Myth of the Technological Fix

Nonspecialists in computer security often expect computer security studies to propose technological solutions, such as encryption, passwords, or automatic audit trails. Although these can be important to a system, in general procedural or administrative measures can improve security more quickly and easily. The "technological fix" has immediate appeal: it is modern, even state-of-the-art; it is technical in a technical system; and, most important, it often doesn't require people to change their behavior. Management, not understanding the full scope of the problem, finds it easy to believe that the solution lies in technology.

However, even with a technological solution, procedural changes will still be necessary in most cases. Computer security experts know that without management commitment and proper administrative controls, any battle to improve security is lost before it begins. Thus, this report will focus on the nontechnical actions that the election community itself must take.

The Saltman report exhaustively examined computer election problems and recommended ways to improve security and reliability. Approximately 10,000 copies of the report were distributed to election officials and others. But most jurisdictions did little to change the election community infrastructure and reward system. In hindsight, it is easy to see why the recommendations were hardly carried out.

Even if such a report gets into the hands of officials who can change the system, there is often little motivation to do so and little understanding of the real issues. People generally avoid thinking about crises and planning to prevent them, since crises generally involve unpleasant assumptions about the adequacy of existing systems and the people in charge of them, questions about who will fund the needed changes, and concerns about the legitimacy of incumbent officials elected under the existing systems.

Changing the way a computer-based voting system is managed is not easy; it generally involves:

o high technology that is probably unfamiliar to local officials, especially those in smaller jurisdictions;

o consulting help, often from vendors, usually at additional expense;

o the prospect of little or no help from the state government;

- spending public money; and
- high-visibility risk, should anything go wrong.

Thus, "if it ain't broke, don't fix it" becomes the maxim.

In most jurisdictions that have made improvements, a rather embarrassing incident has become public, showing the rickety old machine of vote counting with all its faults; it was obviously broke, and the political climate was right for improving computer-based systems. Fixing things when they're broke, under public scrutiny, is more costly and less effective than instituting procedural and technical controls in advance. Nevertheless, with some exceptions, problems generally are corrected only after they become obvious.

In many cases, the computer has actually forced election administrators to reexamine the systems and to improve security and reliability. Often, this reexamination was a result not of computerizing ballot counting, but of computerizing registration or some other aspect of the election process. The effect was the same: the computer was a catalyst to force reanalysis of existing systems (both computerized and noncomputerized) and to make them sounder. Typical improvements include the exemplary pre-election test procedures in Washington State, the uniform setup and test procedures in California, and improved technical computer security in Minnesota.

6. The Captiva Island Workshop

Twenty-six experts participated in a sequestered workshop at Captiva Island, Fla., in February 1987 to discuss computer-based election security and reliability. The attendees (see Appendix A) included federal, state, and local election officials, vendors, consultants, an investigative reporter, technical experts, a political scientist, and a former elected official. Each was invited because he or she could offer some combination of interest, expertise, and influence to mitigate the problems of security and reliability in computerized elections. In a calm atmosphere, participants candidly shared their views of the key problems and explored some solutions in detail.

At an initial plenary session the first morning, five focus papers presented various viewpoints on security and reliability of computerized elections. The focus papers (each of which is reproduced in Appendix B) and their authors were as follows:

o "The Election Administrator's Viewpoint," Marie Garber, administrator, State Administrative Board of Election Laws, Maryland.

o "The Election Consultant's Viewpoint," Robert J. Naegele, president, Granite Creek Technology, Inc.

o "A Computer Technologist's View," Willis H. Ware, senior scientist, The Rand Corporation.

o "The Manufacturer's Perspective," Richard McKay, president, Election Services Division, Business Records Corporation.

o "The Citizen and Political Scientist Perspective," Richard Smolka, publisher, Election Administration Reports, and professor, American University.

During the remaining two days of the workshop, small groups wrestled with the issues raised by the focus papers and the lively discussions following their presentations. On the final morning, the leaders presented the working groups' results to all participants, and everyone had the opportunity to make a concluding statement.

The picture which emerged at Captiva was that of an underfunded, underorganized election community that, with some exceptions, cannot put into place adequate software, hardware, or procedures for proper computer security. The election community has little management knowledge of computer security. The relatively small market discourages vendors from building in security features that the community has, to date, not requested. Few jurisdictions share knowledge. Under these conditions, American elections are, in general, more vulnerable to fraud and error than desirable or necessary.

Many participants at the Captiva workshop felt that it was only a matter of time before inadequate understanding of computerized vote counting causes major problems in an important election. In fact, some experts--referring to another system in which inadequate safeguards led to catastrophe and loss of public confidence--characterized the situation as "waiting for Chernobyl."

Preventing potential problems would require relatively little effort, however, and would pay off in more accurate vote-counting. Consequently, the number of challenges and lawsuits would decline, and public mistrust in the system would not be engendered.

7. Action Areas

The discussions at Captiva Island generated several recommendations to improve the reliability and security of computer-based elections, as detailed below.

Develop Uniform Standards

Minimal standardization is essential to computer security and reliability. As Willis H. Ware said at Captiva, "A lack of standards is antithetical to good computer system security. We can't afford to have each entity doing its own thing--the job is too tough. There must be standards and uniformity."[16]

In the few jurisdictions that have combined programming expertise and management strength, standards would also help in developing systems that will accurately count ballots and stand up under scrutiny. In those jurisdictions, standards would be a beacon of good practice. In the vast majority of jurisdictions, which must rely on commercially available products, standards would greatly reduce the number of problem elections.

Seeing this need, the FEC has been developing voluntary standards for voting system hardware and software. As Roy Saltman stated years ago, "Design and documentation requirements can be imposed on computer programs used for vote tallying to improve their reliability, intelligibility, and capabilities for testing and auditing."[17] Since 1984, the FEC has focused on the most widely used tabulation systems: central and precinct count punch card and optical scanning devices. Paper ballots and mechanical lever machines are beyond the scope of those studies. An effort to develop standards for all-electronic precinct machines got under way in mid-1987. Once it is completed (probably in 1988), the FEC will issue all the standards. Appendix D presents tables of contents from the most recent FEC drafts.

While vendors and an advisory committee of election officials are reviewing drafts of the hardware and software standards, election officials in a few states are already using them. Management guidelines are also being developed for pre-election testing, acceptance testing, and equipment setup and testing.

Although computer security requires standardization, local jurisdictions must abide by their particular legal requirements, and many localities fear externally imposed nonsolutions. Robert Lemens, assistant attorney general and former director of elections for the state of Texas, said, "Harmonization may be desirable to the extent that we may learn from the thoughts and experiences of others. However, our reaction to harmonization is negative to the extent that it can mean abdication of each state's responsibility to address the character of its perceived threats to security in the context of its own legal and administrative structure and its particular political environment."[18]

The FEC and its contractors have encountered other concerns regarding the impact of the proposed standards:[19] they might raise the price of equipment, compromise corporate proprietary rights, inhibit competition by discouraging new vendors from entering the market, inhibit the introduction of innovative systems, and impose an unacceptable burden on vendors and local jurisdictions alike in terms of time and money. However, the FEC staff, vendors, and election officials are working on resolving problems such as these. The security and integrity of elections are critical to democracy, and minimizing fraud and error is extremely important. Guidelines or standards that help to do this are necessary.

Rational, uniform standards can, if properly written, allow adequate flexibility for local elections. And local jurisdictions, whether they buy or develop their own vote-counting systems, need not blindly accept what the vendor's representative offers. They should certainly shop around and demand minimal features for security and reliability, such as those described in the Saltman report and in the forthcoming FEC standards. Locally developed administrative and procedural policies, which may draw from the federal management guidelines, could supplement these measures.

Improve Pre-election Testing

Pre-election tests ensure that the vote-counting equipment tallies votes correctly before the election begins. In general, pre-election tests now leave much to be desired. Sometimes only three ballots are counted! These are not exhaustive tests at all. They do not detect any programming errors. Moreover, they are often conducted by the same vendors who sold the machines. It is not surprising that the systems pass the tests.

Election officials (not the vendors) must perform much more exhaustive testing and should allow time to do so. The Illinois State Board of Elections said it well: "The testing of computer vote tabulation systems needs to be improved substantially. At a minimum, voting systems tests must be large; must test all voting positions; must test overvotes [votes for more candidates for a particular office than allowed by law] and undervotes [votes for fewer than the maximum number of candidates in a multiposition contest]; column binary punches; straight and split party votes; nonvoting position punches; and must test for every candidate in every ballot configuration in every precinct. Only by extensive testing of a computer vote tabulation system can we be reasonably assured that tabulation of the ballots will be entirely accurate."[20]

A source independent of the vendors needs to provide a standard test sequence of ballots or vote images (a "deck") to test much more than the working condition of the ballot readers; it must also test in detail the accuracy of vote counting.

As part of the setup and test process, coding (the setup for a given election) of candidates and voting positions should be done in a formally documented, step-by-step procedure. Each step should be recorded on an audit trail.

The Captiva workshop participants examined one particularly disturbing issue: in a significant number of cases, pre-election testing did not detect incorrect coding for certain elections, necessitating coding changes during the elections. Occasionally, programmers have changed the actual program (not just the coding) after the pre-election test. Sometimes this is done to comply with a court order or to correct a setup that the jurisdiction has belatedly realized will not work. This very important security violation calls into question all counts done by any such program; in these cases, an untested program counted election ballots, because time had not been allowed for proper pre-election testing.

Improve Post-election Review and Audit Capabilities

Post-election review and audit procedures must be improved to guarantee that a recount can be done if necessary. Most systems, whether they use hard-copy ballots or not, were not designed with auditing in mind, and the programming style often reflects practices long since abandoned in modern software development. Moreover, auditing by a hand recount is impossible with some all-electronic systems (older, all-mechanical lever machines are similar), since there is no record of votes on a ballot to recount. Newer systems record each ballot's content and scramble the order. This may provide adequate voter confidentiality while creating an audit trail.

Vendors could, at some cost, provide effectively unerasable audit trails similar to the flight data recorders on airliners. Such records could include what was coded, tested, counted, and validated before, during, and after the election, starting at pre-election setup and testing. These records would include logs of printer, card reader, and other peripheral devices in accordance with the FEC standards.

One might ask, "Why bother keeping an audit trail until you can be sure that the proprietary program itself behaves as it should? And how can you do that if the vendor won't let you see the program?" Some vendors have deposited their proprietary source code in a confidential software escrow account. If necessary, independent experts can examine the software to determine whether it counts correctly and to establish a base point for deciding whether changes have been made that would require recertification or prove fraud. But having outside experts examine the program is very expensive and time-consuming, particularly because contemporary software reflects an old style of programming. To date, software escrow has been rare, but the FEC, as it drafts the voting systems standards, is considering a number of guidelines for software escrow.

Rationalize Assessment, Certification, and Decertification

Currently each state, with its own rules and regulations, tests and certifies computerized election systems. Testing at the state level may actually narrow the selection of available equipment if a vendor does not have the money or personnel to pursue certification in each state. One respected national body might perform the qualification testing (the majority of all testing) more competently and, since it would be done one time only, much more inexpensively. And, indeed, the draft FEC standards point toward a few independent testing authorities (ITAs) funded by the vendors to perform basic qualification testing.

Illinois has designed a sample ballot, intended for high-volume acceptance tests, to provide opportunities for comprehensively testing all possible ballot conditions.[21]

Clarify Responsibilities

The Captiva workshop participants generally agreed that election officials too often delegate responsibility inappropriately or ambiguously. The election official, not the vendor, is responsible for (1) defining (coding) the election; (2) setting up and monitoring the pre-election test; (3) running the election; and (4) processing the appropriate documents after the election. In too many cases, election officials delegate these responsibilities to the vendor, who is more familiar with the computerized system. But the election official, not the vendor, is ultimately accountable. Officials who make the effort to understand computer systems not only protect themselves better, but also probably get better service from the vendor.

Improve Training

Better training is needed for election officials. Even computer experts have difficulty understanding the very precise and highly technical documents often used to describe or specify computer-based vote-counting systems; and laws and regulations are often not presented in crystal-clear prose. It is folly to expect local or even many state officials with limited time and resources to understand documents that too often are written in either "computerspeak" or "federalese."

Of course, vendors provide some training, but as mentioned earlier, local officials often take the easy way out and rely only on the vendor. This does not provide a completely impartial source of information. Some leading states have provided documentation and guidance for their local election officials, but most do not. There is apparently no "cookbook" of procedures, practices, and forms. The Election Center (see Section 8 below) also provides some training for its members, but both it and the FEC reach only a fraction of the officials who should be getting trained. Some experts have suggested that state certification entities also take on the responsibility of training local officials, but they generally don't have adequate resources to do this.

A highly professional training program about computerized voting systems, including graphics, videotapes, and flow charts, might be appropriate for training the election community and for informing others:

o Legislators, who must understand the process to govern and fund it.

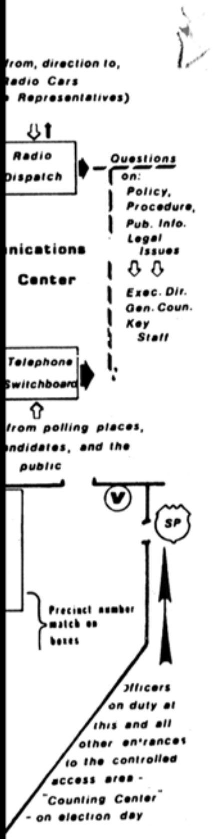
o Election officials, including poll watchers and core and auxiliary staff, who implement the process and define its operation. They should have a clear description of the process, right down to maps of the voting room with arrows showing ballot and voter flow. (Figure 2 shows an example, from the District of Columbia.)

o The media, who deserve better diagrams of the process than flow charts that, according to Emmett Fremaux of the D.C. Board of Elections and Ethics, look like "wars among the ant colonies."

o Candidates and their campaign managers, who have their honor, ideas, and ideals assessed in a fishbowl. Their time is being spent; they deserve the courtesy of an explanation of the process.

o The public, who pays for it all.

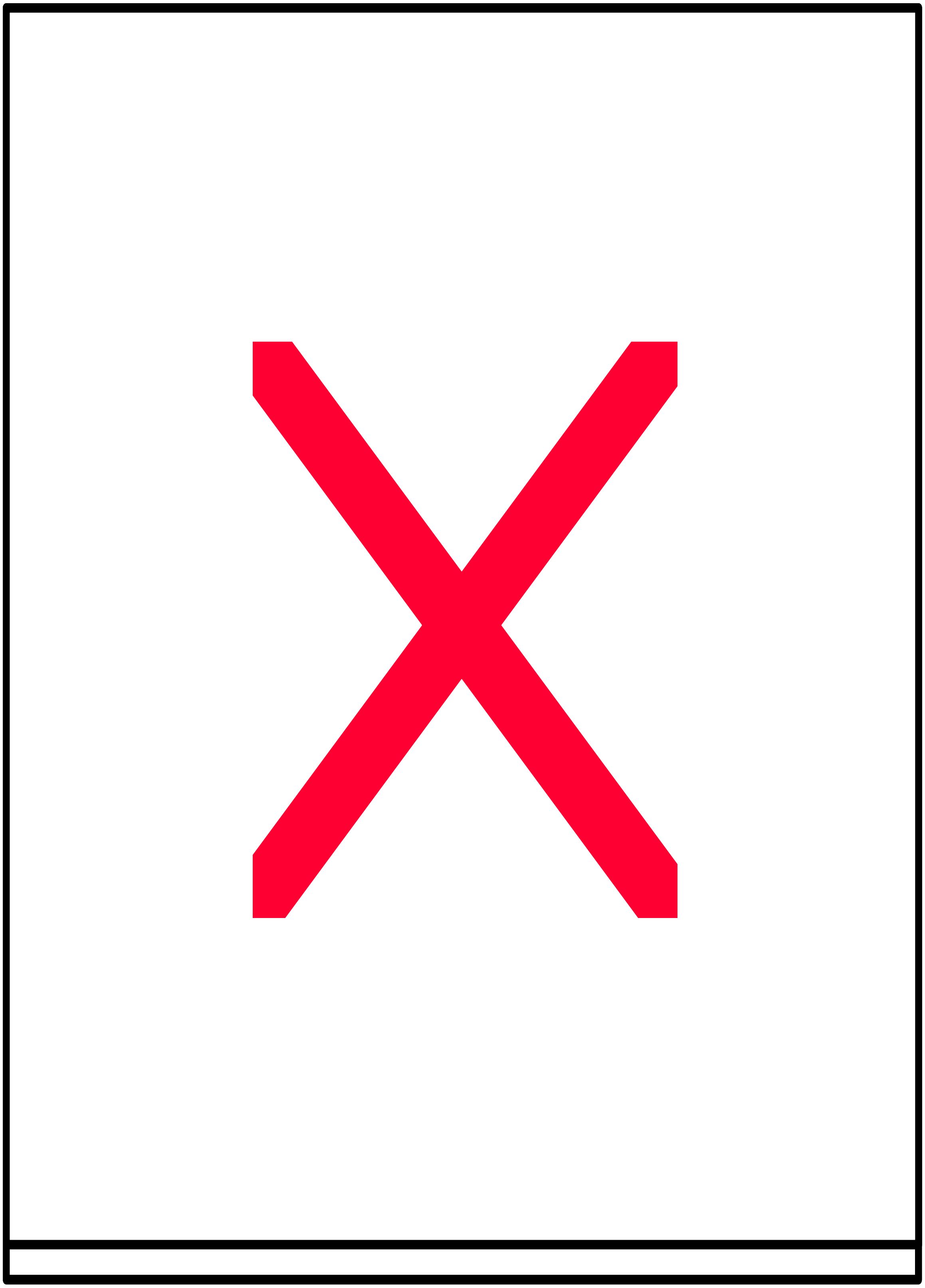
[redacted]



Floor

rd of Elections and Ethics)

Arthur Young & Company, in work sponsored by the FEC,[22] and [redacted]



able to adopt joint positions on matters of common interest to

[redacted]

Actor/Action Matrix

Figure 3 shows the organizations or individuals now working

[redacted]

Page 28a

This is Page 28 (redrawn in Year 2000 to make more legible):

28 MAKING EVERY VOTE COUNT

	FEC	Vendors	Consultants	State Certification Entities	Election Center	National Associations	State Associations	Election Officials	Media	Individuals
Develop uniform standards	x	x	x	X						
Improve Pre-election Testing	x			x				x	X	
Improve Post-election Review and Audit	X							x	x	x
Rationalize Assessment, Certification, and Decertification	x	x	x	x						
Clarify Responsibilities		x		x				X		
Improve Training		x			x	x	x	x		
Standardize Terminology										
Plan for the 1990s										

Figure 3. Actions and Actors Today

original file formats or architectures were open). Individual jurisdictions could buy these software packages, or states or vendor-specific user groups could buy them in bulk.

Special Interest Group on Certification and Decertification

As of 1985, 45 states had installed computer-based voting machines. Most of those have some body to evaluate and certify the machines. Information exchange among these bodies now leaves much to be desired, and a special interest group on certification and decertification could facilitate such exchange. It might also help standardize terminology among the states, maintain a library of reports from each state certification body, and develop common guidelines for the various certifying entities, which are composed of boards, committees, secretaries of state, chief executive officers of the state, or experts, depending on the state.

Special Interest Group on Security and Reliability

A special interest group on security and reliability could provide a forum for exchanging and disseminating information on technical and nontechnical mechanisms for security and reliability. Such a forum is much needed in the election community. As Willis H. Ware has noted, "except for a few large jurisdictions, the state of knowledge for system security, especially in software matters, in the vote-counting community appears to lie between very primitive and nonexistent. Likewise, the operational procedures are not standardized; many jurisdictions probably invent their own. This community is low on the learning curve of security. It has not taken advantage of knowledge that exists elsewhere and is applicable. It is not talking with the communities that are handling reliability, integrity, and security well."[29]

Sophisticated technical threats are probably relatively unimportant in election systems. But good computer security requires safeguards not only in technical areas of communications, hardware, and software, but also in administrative and management controls, operational procedures, physical arrangements, and personnel screening. These nontechnical safeguards are usually easier to implement and less expensive; collectively, they can afford a relatively high measure of protection.

The members of this special interest group--vendors, technical staffers, and concerned staff members without specific technical expertise--may wish to share costs and ideas in developing common controls and procedures. For example, the group might develop an accepted industry standard for randomizing ballot images in all-electronic systems. When and if network transmissions increase greatly, the group might work on the application of cryptography or error-correcting codes to elections.[30]

Coverage of All Needed Actions by Revised Actor/Action Matrix

Figure 4 shows how the new players proposed above would fit into the actor/action matrix of Section 8. With these new players, every needed action could be carried out, and the security and reliability of elections would be considerably improved.

	FED	VENDORS	CONSULTANTS	STATE CERTIFICATION ENTITIES	ELECTION CENTER	NATIONAL ASSO-CIATIONS	STATE ASSO-CIATIONS	ELECTION OFFICIALS	MEDIA	INDIVI-DUALS	VENDOR-SPECIFIC USER GROUPS	SECURITY AND RELIABILITY SPECIAL INTEREST GROUP	CERTIFICATION AND DECERTIFICATION SPECIAL INTEREST GROUP	VENDOR GROUP
Develop Uniform Standards	x	x	x	x								x		
Improve Pre-election Testing	x			x				x	x		x	x		x
Improve Post-election Review and Audit	x							x	x	x	x	x		
Rationalize Assessment, Certification and Decertification	x	x	x	x								x	x	
Clarify Responsibilities		x		x				x	x			x	x	
Improve Training		x			x	x	x	x			x	x		x
Standardize Terminology													x	x
Plan for the 1990s												x	x	

Figure 4. Desirable Actions and Actors

Page 32a

This is Page 32 (redrawn in Year 2000 to make more legible):

	FEC	Vendors	Consultants	State Certification Entities	Election Center	National Associations	State Associations	Election Officials	Media	Individuals	Vendor-Specific User Groups	Security and Reliability Special Interest Group	Certification and Decertification Special Interest Group	Vendor Group
Develop uniform standards	x	x	x	X								NEW		
Improve Pre-election Testing	x			x				x	X		NEW	NEW		NEW
Improve Post-election Review and Audit	X							x	x	x	NEW	NEW		
Rationalize Assessment, Certification, and Decertification	x	x	x	x								NEW	NEW	
Clarify Responsibilities		x		x				X	NEW			NEW	NEW	
Improve Training		x			x	x	x	x			NEW	NEW		NEW
Standardize Terminology													NEW	NEW
Plan for the 1990s												NEW	NEW	

Figure 4. Desirable Actions and Actors

10. An Umbrella Organization for the Election Community

None of the organizations described above provides technological knowledge, long-term institutional memory, or education/outreach sufficient to adequately improve security and reliability of computerized elections. This is not surprising, since they are national organizations, and U.S. elections are primarily locally organized. The autonomy of local and state entities, however, inhibits sharing technological knowledge and learning from the successes and failures of others. An umbrella organization would bring together election officials, users, vendors, consultants, and political scientists to promote their common interests and would raise the level of professionalism in election administration.

This umbrella organization (nicknamed "Friends of Elections" by the participants in the Captiva workshop) would be a repository for knowledge and enable informed individuals to transmit that knowledge to their fellows. It would recognize and reward outstanding accomplishment in election administration, foster the adoption of minimum standards in this area, and enable its members to interact regularly. It could initiate projects or cooperate with others and could encourage, fund, produce, endorse, or disseminate the results.

For example, a new Illinois sample ballot surpasses the traditional "test decks" in pre-election testing for anomalies in vote-counting programs. If other jurisdictions knew of it, they might be able to adapt it to their own elections, greatly improving their pre-election testing at a relatively small cost. However, no one outside Illinois received it, except some Captiva participants (a de facto "Friends of Elections" organization) and ECRI (a nonprofit testing and research institute near Philadelphia, which may use the ballot in voting machine tests [see Section 11]). The reason is simple. There is no effective, appropriate, informal, easy-to-use, timely communication channel to deliver work in progress to the majority of the election administration community fast. The umbrella organization could easily provide one.

One model for this is the Association for Computing Machinery (ACM), a professional organization for computer analysts, programmers, and educators. Its annual dues fund Communications, a monthly magazine for all members. It has one annual meeting; regional chapters typically have monthly meetings; and numerous special interest groups have additional dues, publications, and conferences. The Council of the ACM, its governing board, allocates money for demonstration projects and special interest groups, which allows members with specific interests to visit other members to work on shared interests and encourage support. In the process, experts on specialized topics emerge and become recognized within the organization and the professional community.

"Friends of Elections" could provide an incentive for vendors and consultants to work together on projects that would benefit all and reduce overall costs in the long run. Today, without the funding and cachet of a professional organization, vendors have more incentive to concentrate on profitable activities and shun work toward the common good. A proposal coming from only one source can be easily construed as biased; if a professional organization with knowledge and clout received the same proposal, examined it thoroughly, critically reviewed it, revised it appropriately, and then put it forth as the position of the organization, it would have a much better chance of being implemented. It would also serve as a de facto guideline for the election community, much as the Generally Accepted Accounting Principles do in accounting. Moreover, because many people would have been directly involved in drafting the proposal, it would have more support at the various jurisdictional and legislative levels.

Agreement in the election community to take the actions recommended in Section 7 would hasten significant security and reliability improvements. But the election community has been so diffuse and unorganized that inertia has prevented significant progress in these areas. Election officials tend to react to problems after they occur rather than anticipate them and devise solutions. An incentive system that rewards election officials for improving security and reliability would be less expensive in both dollars and goodwill in the long run. An umbrella organization, by institutionalizing such an incentive system with peer recognition and benefits, would be a step in that direction.

Organization

At start-up, "Friends of Elections" could be staffed in one of three ways:

o By a full-time or part-time executive director (not necessarily an election official) who would ideally be comfortable in the worlds of public administration, politics, and technology.

o By an association management firm with similar characteristics.

o By a part-time, donated staff (such as the staff in the office of an elections administrator).

The first or second options are more desirable. They permit clear definition of measurable goals, and the person in charge can be rewarded relative to how well he or she meets those goals.

They remove the question of bias toward one type of election official or office. Moreover, a handful of people with expertise in election administration and the respect of their peers might be available and interested in taking on this challenge to add to their accomplishments in the field.

For appropriate cachet and support, the organization should have an influential board of governors: nationally recognized election officials; politicians or former politicians; chairmen of the two major national parties; top-notch chief executive, operational, and financial officers; vendors; political scientists; and computer scientists. It should be located in a prestigious location in Washington, D.C., to take advantage of proximity to the FEC, other administration offices, Congress, and many other participants in election administration.

Role

An umbrella organization should provide a ladder of community-wide recognition and prestige to climb, and could furnish a framework for working on topics of special interest to leaders in the election community. The Election Center or the FEC Clearinghouse might be able to carry out some of the recommendations in Section 7, but for either organization to implement them all, it would have to redefine its mission, undergo massive restructuring, and receive a large infusion of new resources.

A new organization could support several special interest groups from the start. In particular, the missing players described in Section 9 could be special interest groups of the umbrella organization. In fact, the organization could include special interest groups corresponding to each of the recommended areas of action: standards, pre-election testing, auditing, certification, responsibility assignment, training, terminology standardization, and planning. These could all be fused together by the new organization into an ongoing, coherent structure driven by the needs and interests of individuals in the election community. This would improve not only security and reliability, but also many other aspects of election administration.

Funding

The organization must be built and perceived as nonpartisan, skilled, professional, and, most important, capable of delivering something of value. Obtaining many start-up memberships from a group as fragmented and impecunious as the election community is not feasible. Instead, multiyear funding from government or foundation sources will be necessary, until the organization establishes a reputation for products that are worth the membership fee.

State governments may provide some funds, particularly if they see that the organization can provide benefits in training, certification, and other areas of common concern. Even a small increase in the FEC Clearinghouse budget, if used as seed money, could prove very effective.

11. Areas for Further Study

Some important projects in computerized elections have started recently. In addition, this study identified several worthwhile topics that were outside its scope or that were not researched because of time constraints. This section briefly describes them.

Updated Guidelines for Administering Computerized Elections

At the National Bureau of Standards Institute for Computer Science and Technology, Roy Saltman is studying the current state of computerized voting systems, taking into account the technological changes since his 1975 report. His objectives are (1) to provide public officials with guidelines on the management and use of computerized systems, promoting smoothly run, accurate elections, as well as ensuring security of the process and the confidentiality each voter's choices; (2) to review the technical aspects of recent election difficulties involving computers, clarifying the problems and recommending ways to avoid similar problems in the future; and (3) to aid in developing a neutral source of technological expertise for election administrators and others concerned with the accuracy, security, and effective execution of elections. Saltman will publish a new report and conduct a series of workshops for election officials.

Election Official's Guide to Computerized Voting Systems

ECRI, a nonprofit research and testing organization, is conducting a engineering, computer science, and human factors analysis to compare and evaluate the electromechanical and electronic voting systems now available. The final report will be a "consumer's guide" to aid election officials in future acquisition decisions. Malin Van Antwerp is directing the project at ECRI's Plymouth Meeting, Pa., headquarters.

Model Contract and Request for Proposal

A model contract and a model request for proposal based upon the upcoming FEC standards are currently being worked on by the FEC Clearinghouse, and a draft should be available in December 1987. If these are developed and used, they should result in significant savings for vendors and, ultimately, purchasers, since they would reduce the efforts each must make during the purchasing process.

How and Why Some Jurisdictions Have Improved

A few jurisdictions have improved significantly since the Saltman report was issued. Their election systems should be examined in detail to discover how and why they improved. The manifestation of the original problems, the expectations of the problem solvers and others in the community, and the outcomes of various actions should all be examined, in the hope of finding common lessons.

12. Conclusions and Recommendations

As mentioned above, the election community is underfunded and underorganized. With some exceptions, it knows little about managing computer security. Few jurisdictions share knowledge. Thus, American elections are more vulnerable to fraud and error than desirable or necessary.

Preventing most potential problems will take relatively little effort, none of it highly technical. What can and should be done has been discussed above. The first seven recommendations can be acted upon by any jurisdiction. The last three require broad-based action.

Specific Recommendations for Jurisdictions

1. The FEC standards and management guidelines for computer-based vote counting systems should be adhered to as much as possible.

2. Complete post-election review and audit capabilities should be required in all newly purchased or developed systems.

3. State certification entities should exchange information to make that activity as uniform as possible.

4. States should insure that local officials do not inappropriately or ambiguously delegate authority for conducting an election to vendors of vote-counting machines or to anyone else.

5. Training -- practices, procedures, forms, and technical understanding -- should be improved.

6. Existing internal or external auditors should be encouraged to develop additional statements about internal controls to address concerns about the security and reliability of computer-based vote counting systems.

7. Pre-election testing and post-election review and audit should be scrutinized, and improved if necessary.

Recommendations Related to the Election Community Infrastructure

8. Developing an umbrella organization for the election administration community to provide a ladder of professional advancement and recognition should be examined in more depth. Its relationship to existing entities such as the FEC Clearinghouse on Election Administration and the Election Center should be carefully examined to identify potential duplicative efforts as well as unique opportunities available to such an organization.

9. A standard glossary should be developed for the election administration community. Technical specialists should be called upon to help with this as appropriate.

10. Potential problems such as issues of one-vendor dominance, pollworker scarcity or glut, and communications privacy and security should be monitored.

If the above recommendations are implemented in most jurisdictions, the security and reliability of computer-based elections will be greatly improved, as will the election administration process in general.

NOTES

1. George B. Mather, Lost Votes: Effects of Methods of Voting on Voter Participation, Iowa 1920-1984, (Iowa City: University of Iowa Institute of Public Affairs, Division of Continuing Education, 1986).

2. David Burnham, "Texas Looks into Reports of Vote Fraud," New York Times (September 23, 1986): 12.

3. Peter Ellerston, "Moline Election Fouled Up by Computer," Illinois Issues (November 1985): 12-15.

4. Seth Rosenfeld, "Ballot Computers May Not Be Secure Against Tampering," San Francisco Examiner (October 20, 1986): B1.

5. Michael L. Harty and Ricky S. Fulle, Summary of Findings and Observations of the State Board of Elections Computer Testing Program, (Springfield, Ill.: Division of Voting Systems and Standards, August 1987).

6. Michael L. Harty, testimony to the Illinois Senate Republican Task Force on Vote Fraud, September 17, 1985.

7. Roy G. Saltman, Effective Use of Computing Technology in Vote Tallying, National Bureau of Standards Report NBSIR 75-687, March 1975. Order no. COM75-11137 (Springfield, Va.: National Technical Information Service), p. 1.

8. Willis H. Ware, Integrity and Security of Automated Elections: A Computer Technologist's View of the Scene, focus papere presented at Captiva Island Workshop, revised October, 1987 (included in Appendix B).

9. "Agenda for Reform of the New York City Board of Elections", Final Report of the New York City Partnership Task Force for the Board of Elections to the Honorable Edward I Koch, Mayor of the City of New York, June 30, 1985, p. 23.

10. Source: Election Data Services, Inc., 1987.

11. Aubrey Dahl, "Burning Issues at Stake in General Election: So Who Counts?," Datamation (November 1, 1970):48-49.

12. John W. Verity, "Machine Politics: Charges of Vote Fraud and Sloppy Technology Cloud the Role of Computers in the Electoral Process," Datamation (November 1, 1986):54ff.

13. T. Elkins and E. Waskell, "Bugs in the Ballot Box," Campaigns and Elections (March/April 1987):20-25.

14. Committee on Computers and Public Policy, Association for Computing Machinery, "Report for the Computerized Voting Symposium," RISKS-FORUM Digest, vol. 3 (September 20, 1986).

Elkins and Waskell, "Bugs in the Ballot Box."

16. Ware, Integrity and Security of Automated Elections: A Computer Technologist's View of the Scene.

17. Saltman, Effective Use of Computing Technology in Vote Tallying.

Robert Lemens, private communication, August 10, 1987.

19. Federal Election Commission Clearinghouse on Election Administration, Voting System Standards Implementation Plan, undated draft.

20. Harty and Fulle, Summary of Findings and Observations of the State Board of Elections Computer Testing Program.

21. Illinois State Board of Elections, Ballot for Voting System Approval Testing, (Springfield, Ill.: Division of Voting Systems and Standards, 1987).

22. National Clearinghouse on Election Administration, Computerizing Election Administration, vol. 2 (Washington, D.C.: Federal Election Commission, Autumn 1986).

23. Peggy Sims and Bill Kimberling, "All-Mail Ballot Elections," FEC Journal of Election Administration, 14 (Spring 1987):19-22.

24. Election Administration Reports, June 22, 1987, p. 4., 5620 33rd St. N.W., Washington, D. C. 20015.

25. Dorothy Denning, Cryptography and Data Security (1982: Addison-Wesley, Reading, Mass.).

26. Election Administration Reports, August 3, 1987.

27. Ware, Integrity and Security of Automated Elections--A Computer Technologist's View of the Scene.

28. Ibid.

29. Ibid.

30. Denning, Cryptography and Data Security.

Appendix A. Workshop Participants

Bruce Bolinger
County Clerk-Recorder
Nevada County
12704 Butterfly Drive
Nevada City, CA 95959
(916) 265-1293

Penelope Bonsall
Director
National Clearinghouse on Election
Administration, Federal Election Commission
999 E Street, NW, 7th Floor
Washington, DC 20463
(202) 376-5670

Kimball Brace
President
Election Data Services, Inc.
1522 K Street, NW, Suite 626
Washington, DC 20005
(202) 789-2004

David Burnham
Writer
122 Maryland Avenue, NE
Washington, DC 20002
(202) 546-3716

Herb Deutsch
Vice President
BRC Election Services
328 S. Jefferson Street
Chicago, IL 60606
(312) 454-1471

Emmett Fremaux, Jr.
D.C. Board of Elections and Ethics
1350 Pennsylvania Avenue, NW, Room 4
Washington, DC 20004
(202) 727-2525

Marie Garber
(Former Administrator-State
Administrative Board of Election Laws)
10409 Hutting Place
Silver Spring, MD 20902-4951
(301) 933-0996

Paul Goldy
President
International Technology Group
877 Kings Highway
Woodbury, NJ 08096
(609) 848-3627

Michael Harty
Director
Voting Systems and Standards
Illinois State Board of Elections
1020 South Spring Street
(P.O. Box 4187)
Springfield, IL 62708
(217) 782-1569

Ralph Heikkila
Assistant Registrar/Recorder
Technical Services, Los Angeles County
5557 Ferguson Drive
(P.O. Box 30450)
Los Angeles, CA 90030-0450
(213) 725-5666

Lance J. Hoffman
Professor
Department of Electrical Engineering and
Computer Science
The George Washington University
Washington, DC 20052
(202) 994-4955

Helen Koss
(Former Member - Maryland House
of Delegates)
3416 Highview Court
Silver Spring, MD 20902
(301) 942-9091

Robert Lemens
Assistant Attorney General
State & County Division, State of Texas
1124 South 1H35
(P.O. Box 12548)
Austin, TX 78711-2548
(512) 463-2120

Richard McKay
President
BRC Election Services
328 S. Jefferson St.
Chicago, IL 60606
(312) 454-1471

Jacob Merriwether
Vice President
International Technology Group
877 Kings Highway
Woodbury, NJ 08096
(609) 848-3627

Robert J. Naegele
President
Granite Creek Technology
400 Linda Vista Drive
La Selva Beach, CA 95076
(408) 728-4244

Paula Newberg
Program Officer
The Markle Foundation
50 Rockefeller Plaza, #940
New York, NY 10020
(212) 489-6655

Roy G. Saltman
Computer Scientist
National Bureau of Standards
A-266, Technology Building
Gaithersburg, MD 20899
(301) 975-3376

Deborah Seiler
Assistant to the Secretary of State
Elections and Political Reform
1230 J Street
Sacramento, CA 95814
(916) 445-0820

Michael I. Shamos
President
UNILOGIC, Ltd.
Commerce Court, Suite 240
Four Station Square
Pittsburgh, PA 15219-1119
(412) 281-5959

Larry Slesinger
Program Officer
The Markle Foundation
4912 45th Street, NW
Washington, DC 20016
(202) 966-3204

Richard Smolka
Editor
Election Administration Reports
5620 33rd Street, NW
Washington, DC 20015
(202) 244-5844

Mary Stone
(Former Deputy Administrator of
Elections, Montgomery County, Maryland)
10610 Glenwild Road
Silver Spring, MD 20901
(301) 429-1965

David Stutsman
Senior Partner
Stutsman, Stevens, Leone & Clifford
216 South Fourth Street
(P.O. Box 100)
Elkhart, IN 46516
(219) 295-7175

Robert D. Tyre
Business Records Corporation
7800 Stemmons Freeway
Third Floor
Dallas, TX 75247
(214) 905-2315

Willis H. Ware
Corporate Research Staff
The RAND Corporation
1700 Main Street
(P.O. Box 2138)
Santa Monica, CA 90406-2138
(213) 393-0411

Douglas A. Webb
Senior Management Systems Consultant
SRI International
333 Ravenswood Avenue, BS-243
Menlo Park, CA 94025
(415) 859-5224

Frederick Weingarten
Program Manager
Office of Technology Assessment
U.S. Congress
600 Pennsylvania Avenue, Suite 309
Washington, DC 20510-8025
(202) 226-2249

Appendix B. Focus Papers presented at the workshop

THE ELECTION ADMINISTRATOR'S VIEWPOINT

Marie Garber[1]
Administrator, Maryland Administrative Board of Election Laws

In considering computer-based vote-counting systems, the election administrator's major concern is that the system will work. Before the system is installed, the election administrator and the public must be satisfied that it will work. After the election, the election administrator must demonstrate, both to his or her satisfaction and to the public, that it has worked.

The vendor may supply the pre-election test, or the customer may have to devise it. In either case, the test must be comprehensive. It must ensure proper logic and accuracy and account for ballot styles and rotation. The test must be extensive enough to simulate an actual election, and at least part of the test should use actual ballots. The question that must be answered is, "How can we explain to the public that the test does indeed demonstrate the reliability of the system?"

Post-election verification entails demonstrating that the system which tested correctly before the vote counting started still counts correctly and has not been altered. Roy Saltman has suggested getting closer to a 100 percent recount as the election approaches a tie, but a 100 percent recount is an enormous job.

The ballot document itself is important. Reliability is not always a matter of hardware and software. The printing must account for tolerance limits for registration and for space constraints. Weight, color, grain, and moisture-resistance must be considered in choosing the stock. Also, the capacity of the ballot and the effect of folding must be taken into account. One must investigate whether the ink or stock affects the ability of the machine to read the document.

The election administrator must know whether the document reader counts every ballot, whether it indicates that it has not counted a ballot, and whether it identifies the ballots it has rejected (and why it has rejected them). The availability of standard card readers, for central counting of a large volume, is another issue that must be considered.

The election official must be in charge and take responsibility for security. One is always faced with the dilemma of a "cocoon" (limited access) versus a "fishbowl" (an open count). One must ask, "Can the system be corrupted? If so, where?" Other important security issues include online reporting of results during the count and the election official's

[1] Current address: See Appendix A.

dependence on the vendor for the vote-counting program coding and the creation of the memory pack.

Proper documentation of the process is necessary. Does the system automatically record everything that happens and preserve this record for post- election examination?

Election administrators are now faced with the choice between microcomputers and mainframes. Until recently, mainframe was the only choice. Now all but the large election agencies use microcomputers. The advantages of the mainframe are that its maintenance is constant and reliable and that it fully documents and prints out all transactions. However, because it is sometimes difficult to dedicate the system for vote tallying, the administrator risks access by an outsider during vote counting. On the other hand, the microcomputer is a dedicated system and eliminates the risk of unwarranted access, but presents drawbacks in maintenance: the election agency doesn't have the staff in-house, the vendor may not be available, and contracting with a local service organization is difficult. Also, the micro is not as likely to document and print out all transactions.

Marking devices, too, have their own unique advantages and disadvantages. Pencil/pen systems are simple and cheap, but some kinds don't read well. For punching devices, one must consider the tolerances in the placement of the card.

Nondocument systems pose an enormously important question: how can one recount and thereby confirm that the original count was correct?

Election administrators face special problems with respect to precinct tabulators. The polling place equipment is expensive, and there is probably no backup. Testing and setup is a large volume job. Other issues include capacity of the ballot receptacle, securing ballots after the polls close, transmitting the precinct count to the central office (either over a phone line or hand carried), and machine aggregation.

Finally, staffing is a concern of election administrators. The election administrator, who is not a technician, is in charge of a highly technical computer staff. How much in-house expertise, either in the election office or in general government, is required to effectively manage a computer-based voting system? Do small communities have that expertise? Do small states have the expertise to examine and certify systems or to police their use by localities? Do different types of systems require different kinds or degrees of expertise?

SECURITY AND RELIABILITY OF COMPUTERS IN ELECTIONS: THE MANUFACTURER'S PERSPECTIVE

Richard H. McKay
President, Business Records Corporation
Election Services Division

Introduction

All ballot tabulation manufacturers recognize that ballot security is a priority in the minds of voters. Every person who casts a ballot is concerned that vote totals are correct. So, while manufacturers have a direct involvement in the integrity of the ballot box, they readily acknowledge that security is everybody's business.

Business Records Corporation manufactures three types of vote counting systems and associated equipment. This includes punch card, optical scan, and full electronic. Generally speaking, the company now manufactures equipment for every type of system on the market. There are other manufacturers who produce equipment which is similar in concept but built to varying degrees of complexity and specifications. All new ballot tabulation equipment generates a computer count as a primary or secondary method. Each program is unique for each election, but differs in software specifications, audit trail abilities, program designs, and capabilities. While outputs appear similar, the methods of producing totals varies from device to device.

As the "INDUSTRY SPOKESMAN" I, therefore, want to discuss the security and reliability of computers in elections from a general standpoint rather than refer specifically to a piece of equipment or particular method or system. It is not constructive to focus on one type of equipment because over the years we have seen problems in every type of tabulation system involving paper ballots to the most sophisticated computerized system. Any claims of inappropriate handling and faulty equipment somehow become a reflection on all equipment which is on the market today.

A special problem that is plaguing the computer industry is the claim of vulnerability of computers to being accessed. The hackers who have managed to penetrate bank, credit card, and other computers have created an awareness that this type of thing CAN happen in elections. In my opinion, that is the primary reason why we are here today.

Manufacturers and vendors of counting equipment want to assure their users that the equipment which they market functions accurately and reliably. All manufacturers want the integrity of elections to be above reproach. No one wants their system to be the target of misinformation, mistrust, or law suits. We, therefore, welcome this unique opportunity to participate in a forum which brings together a group of experts who can objectively define the real issues and help with solutions that will guide all of us into a more secure future.

Defining Common Problems

The past two decades have brought to light all types of real and perceived problems, especially for the computerized vote counting devices. The problems have been far-ranging including improper hardware setup, coding errors, and poor systems management. The most frequent and severe problems seemingly are caused by lack of understanding of operating procedures. Recently there have been claims of "possible tampering" and fraud. The result has been in-depth investigations into causes and effects. Governmental investigations have proven beyond a reasonable doubt that most problems have not resulted in overturned election outcomes. More important, the investigations have shown that no tampering or manipulations whatsoever has occurred. Rather, most election problems are the result of archaic laws, lack of management procedures, lack of proper preventative maintenance, improper ballot handling, poor processing of ballots, election coding not matching ballot layout and in larger systems, coding not being consistent between system sections.

Other types of situations occur which have no direct effect on voting outcomes but are problems which may delay the count. Delays may be caused by a variety of circumstances including header cards being improperly punched, coding mistakes, improper ballot handling, and a host of environmental factors. While such errors cause all of us painful headaches, they do not result in dishonest elections. Unfortunately, when the counting process is delayed for any reason, someone is always suspicious of "foul play."

When we strip away the defined problems from perceived problems, we begin to see the possibility that manufacturers have been lax in educating their customers. It is also true that local election officials frequently change. In any case, the education process is not always ongoing at the local level. The culmination then is the need for better informed users armed with minimum standards for control and security. Manufacturers should supply adequate handling and storage information to include training, testing, and environmental influences and their effect on the hardware and software. Accordingly, the need for more and tighter security is not predicated on any manufacturer's poor systems design, rather it is for more protection and proof of proper handling thereby generating greater voter confidence.

Computer Security - Where Does it Begin?

The issue of computer security weighs heavily on the minds of Congress as well as all of us. For that reason, a significant amount of federal funds have been appropriated in the past to study the problems involved and most recently to develop voluntary standards for vote counting devices. Every election equipment manufacturer I am sure, will want to comply with these new industry standards.

The objective of hardware and software design is to produce devices, programs and procedures that can be easily secured, tested, analyzed, used, and understood by the customer. The new Federal Election Commission system standards will be a good yardstick for the future. Many of the suggestions contained in the voluntary standards have already been incorporated or will be incorporated into new products.

All during the designing and manufacturing phases, manufacturers must exhaustively test the hardware and software to determine the possible areas of vulnerability. Based on test results, administrative procedures can be specifically designed to find and overcome possible weaknesses. Manufacturers should naturally become more aware of their systems' potential problem areas and be prepared to alert the users to all necessary security procedures. Manufacturers' testing should also include handling, storage, movement of equipment, and environmental factors which might have an impact on the operation and integrity of the system.

Today's software must contain built-in security measures which include audit reports, time logs, self-testing methods, and error reports. In addition, some manufacturers further protect their program code sources by escrow or placement under lock and key with the users. This issue has caused a great deal of discussion among challenge groups with no discernable conclusions. I am sure all manufacturers would welcome definitive suggestions on this issue.

The present built-in security measures are probably only a fraction of what would be done, but the issue of what else and at what cost weighs heavily on the minds and budgets of everyone concerned. While we want to ensure the integrity of the equipment, there are less technical and more pragmatic issues which would be valuable to address which can further secure the systems.

One of the biggest computer reliability problems that faces an election authority is a result of election data coding not being compatible with the ballot layout or erroneously defining the election. This can occur whether the election is coded by a manufacturer or by the user. The causes can include transcription error, miskeying of data, incorrect certification of data or printing of ballot pages in error. The result, depending on when it is discovered, can be inconsequential if caught at or prior to public test or disastrous if caught after election results are released, especially if by an astute press. The latter situation has, in fact, resulted in accusations of tampering and fraud. Proper procedures and testing prior to, during, and following the tabulation process can alleviate most of these situations.

Manufacturer vs. User Responsibility Proactive vs. Reactive Response

One of the great concerns of the industry is the demand to solve nonproblems caused by misinformation or accusations based on false assumptions. All manufacturers would like to be assured that when they make research and development investments, the users really want and need the new or enhanced products. There are many factors affecting the election process which the industry should acknowledge.

1. Manufacturers and users have not adequately anticipated potential problems, both real and perceived;

2. Manufacturers have not developed and published minimum security guidelines for equipment use;

3. User training often has been deficient as well as support and update training by manufacturers;

4. Manufacturers frequently have not set standardized procedures for equipment use;

5. Users, in general, lack appropriate funds to update systems on a timely basis;

6. Manufacturers often erroneously assume that users are properly trained.

All manufacturers would undoubtedly agree that improved ballot security can begin from better, more intensive user training focusing on handling; testing and securing the equipment; and testing each election setup for correct coding of election information. Improved written materials can be easily developed but this cost would have to be reflected in the price of systems and ultimately borne by the user. The real issue then is how much training, at what cost, and how do we, as manufacturers, make certain that our recommendations are implemented? We have no authority to make our customers follow necessary procedures short of warranty expressions.

Each of the following factors are links in the chain of security which need to be addressed by both the manufacturer and the user when evaluating new voting system alternatives.

Performance and Capacity

* response time
* speed
* memory retention
* expandability re: number of parties and positions

Reliability, accuracy and diagnostics

* weaknesses
* impacts under hostile conditions and environmental problems
* machine integrity

Security

* access to computer
* ballots handling and control
* operation and repair election day

Durability

* useful life
* degree of abuse

Vendor support and service

* independence from manufacturer for coding and maintenance
* spare part availability
* ease of repair

Human factors

* skills needed
* mean time to repair
* election worker integrity

Price/Performance

* cost/benefit

It has been customary for manufacturers to assume partial responsibility for "product liability" whenever the performance of products has been questioned. Philosophically speaking, however, what is the manufacturer's liability if equipment is mishandled by the user, election information is miscoded by the user, or programs or equipment are even penetrated by a conspirator?

Education - How Much the Public, Press and Participants Should Know About the Counting Process

While the election process is increasingly dependent upon technology, we must also be aware that many criticisms and fears are based on probability, possibility, and what ifs. Someone must educate those who deal with the voting and reporting public. Is that a manufacturer or user responsibility? If manufacturers do the educating, they are often accused of self-interest or "only telling the public what they want them to know." Many local administrators do not have the money, the time or the staff to implement an effective public information program. Manufacturers could help by producing manuals, information packets, provide speakers, do public service training, and provide videos about the specific equipment. While added cost would be attached, this may be helpful to promote public awareness and build confidence in new and updated voting systems.

Increased public education may help alleviate the fears, questions, and promote public confidence, but we must anticipate situations where still further measures should be considered.

Independent Contractors as a Buffer Between the User and the Manufacturer

The use of independent contractors frequently has been employed by jurisdictions who have wanted an additional layer of assurance. Such contractors have conducted pre- and post-election analyses and written reports indicating that all reasonable measures were taken to protect the integrity of the process and that the final count is true and accurate. In addition, some of these reports set strict hardware and security guidelines to be followed during all phases of the vote counting procedures.

Manufacturers are always supportive of this type of independent analysis especially since the system itself has been shown to be performing properly. The real question here is at what point a local official should feel that they must call for an independent audit -- and realistically, how many jurisdictions can afford them? If all recommended procedures are being followed and all program testing is done, should a user feel obliged to expend the extra funds?

The Future

The goal of most manufacturers is to produce state-of-the-art equipment that is reasonably priced, easy to operate and updatable or replaceable at a cost an average jurisdiction can afford.

Many issues have arisen concerning implied misuse or improper handling which seem to stem purely from technical terminology and industry jargon that is used by computer experts or non-election persons. For example, it has been said that certain types of computer language, the structure and the speed of a program can affect the integrity of the election. In terms of analyzing problems, manufacturers do not generally agree with such assumptions but can definitely update programs if this causes real concerns. As with other issues, we want to take a long, hard look at the cost versus the effect to make sure when it is worthwhile to users for software to be revised into a more modern mode.

Computer Industry Security Standards

In general, we should be assured that the election computer industry conforms to all acceptable computer industry standards. We should look at what these standards are, how they can be applied to elections, and most importantly, what their implementation will accomplish. When we look at alternative methods, we must be assured that we will improve productivity, improve security, enhance performance, assist in the understanding and management of the system, and above all else, improve the integrity of the process.

Conclusions

On the basis of the new hardware and software election products that we see appearing on the market, it is clear that manufacturers are developing systems that are easier to use, therefore reducing the chance of error.

Perhaps, the major conclusion we can draw for now is that problems do arise caused mainly by mishandling and misunderstanding of the equipment. Many minor problems have been exaggerated by accusations of impropriety, collusion, and conspiracy. We must be sure that when we seek to solve problems, that we do not overreact. If manufacturers have real system deficiencies, they will want to correct them.

In the future, the industry should work more diligently to:

- learn from experience and anticipate problems
- provide minimum security standards for systems accessibility and use
- better educate the users and the public
- expand in-house design testing procedures
- recommend user test and administrative procedures to disclose election coding errors
- conform with FEC standards for security as well as structure, where applicable.

State and federal voting procedures need to be strengthened to include:

1. Equipment maintenance standards developed in conjunction with the manufacturers;

Testing of software and coding as generated for every election in each jurisdiction;

Greater involvement in training and direct participation in computer and equipment testing by impartial third party observers - media, party representatives, et al.

As manufacturers of equipment and designers of software, we look forward to the findings, comments, and recommendations of this group. We are anxious to have problems more clearly defined and appropriate solutions outlined.

COMPUTER ELECTION SECURITY AND RELIABILITY: AN ELECTION CONSULTANT'S VIEWPOINT

Robert J. Naegele
President, Granite Creek Technology, Inc.

Introduction

As an engineering consultant, I try to be an engineer first and a consultant second. Let me tell you what I think my responsibilities are, and what I think I can contribute.

An elections consultant should help make an election a success, whatever that means. When I was learning to fly an airplane, student pilots were told that any landing you could walk away from was a successful landing. Of course, life isn't really that simple; otherwise, an election might be deemed a success if, regardless of all else, no one challenged the result. I think we would all agree that there is more to a successful election than dodging the bullet. A consultant can't make life any less complex, but he can help by reducing the overall complexity to manageable proportions, by peeling away the onion one layer at a time, meanwhile checking each layer to see if it looks healthy.

As an engineering consultant, I would consider an election to be a success if, as a minimum,

> All stocking of materials and readiness tests of equipment were completed in time for orderly distribution and setup at the required locations.
>
> Personnel to operate the equipment and support other election functions were properly trained and available in sufficient quantity when needed.
>
> All tests required to demonstrate readiness for ballot counting were successfully completed on schedule.
>
> All equipment was operated without malfunction throughout the entire period of voting and ballot counting or, in the event of malfunction, repairs were made without any perceptible delay or adverse effect.
>
> Polls were closed and output reports were obtained in a timely manner, without incident or error.
>
> Subsequent manual count of a statistically significant number of ballots verified machine totals exactly.
>
> It was known with virtual certainty that at no time during any of the preceeding was the integrity of the system

compromised by any unauthorized or unlawful act, and a record of this integrity was obtained and preserved.

Of course, there is a lot more to an election than what I have enumerated. These are the simply the areas where an engineer can be effectively used as a consultant.

How a Consultant Sees Things

I hope the remainder of these remarks does not bore you by telling you things that you already know. Some of what I consider important may surprise you or seem trivial. If this is the case, I hope I can convince you that these things really do matter. You can take me with a grain of salt. Please take them seriously.

As many of you know, I have been working with elections hardware since the early 60s. I have observed and audited elections in several states and I don't envy you who have to go through them on a regular basis.

As a consultant after the fact, I have seen a lot of problems which could have been avoided and errors which should have been detected and corrected before it was too late. The reason why they weren't is obvious: the elections environment is so hectic that they were obscured by the tide of events.

Problems and errors form patterns and they persist. Some say, with appealing simplicity and much common sense, "If it ain't broke, don't fix it." You buy along with that concept the risk of receiving a very nasty surprise when you can least afford it. I say, "You won't know if it's broke unless you try to use it, and you better not try to use it unless you know it ain't broke." That concept presents a problem because it is circular, but you can exit the loop by doing the best possible job of analysis and testing before every election, on every bit and piece of the entire system, until you are very sure that "it ain't broke". Then, finally, you can use it. This is like the "Test-Fix-Retest" loop followed in product development, and it should be continued until no more errors can be found under the most stringent test conditions which your resources permit.

How can you tell if the system is broken? If it is broken badly, something will get your attention. If it isn't really broken, only sick, you may not know. There is an etiology of elections failures, accumulated through lessons learned in elections and elsewhere. Look for the symptoms.

As a consultant before the fact, here is where I look:

<u>Hardware</u>: Any evidence of weakness in design, performance, and reliability is cause for concern. Single point failures

are deadly. Failures undetected by the system itself are even worse. I look for both types by doing a Failure Modes, Effects and Criticality Analysis on all data-critical circuits and components.

Component selection and application is important, and some vendors try to keep costs down by using commercial grade components everywhere. This is both short-sighted and dangerous. Commercial-grade components in critical application areas such as A/D and D/A converters and RAM may lead to very high failure rates. All electrical components should be suitably de-rated for their applications.

Immaturity of design and development is evidenced by PC board patches such as jumpers, cut traces and piggybacked ICs. Poor maintenance and faulty preparation are indicated by such things as dust in the path of optical reader heads, glazing on the surface of friction drive components, and maintenance and repair workmanship quality noticeably below that of the original manufacture. Lack of documentation or documentation which does not reflect the equipment configuration suggests that there may be some cracks for things to fall into.

Individually, these attributes and events are seldom fatal, but you seldom find them individually. They usually occur as a pattern and, fatal or not, they are serious enough to degrade the reliability and performance potential of the system.

> Solution: Adherence to good design practice, a thorough design analysis before committment to production, and in-house testing to validate component selection and application. To catch residual deficiencies, rigorous and uniform Certification testing, tough Acceptance testing by users, and definitive requirements and provision for the best possible operational and logistical support.

<u>Software</u>: For reasons which elude me, elections software seems to be privileged, so arcane and holy that only the priesthood of programmers can know it and the laity must accept the word as handed down by the output printer. I will accept that when there is an RS-232C interface for stone tablets. Up until now at least, software is above and exempt from constraints on language and structure, and from the kind of analysis and testing which elections hardware has been subject to for a quarter-century.

A lack of visibility into software design and operation has been the rule, making it difficult if not impossible for users to do an adequate job of integrating hardware and software, and of integrating vendor- and user-supplied software packages. Looking for visibility and finding none, I conclude that there must be a good reason for obscurantism. I then prescribe a lot of testing which may in any given instance be unnecessary. What are the alternatives?

As with hardware, the effective integration of all functional requirements is the goal. The absence of integral security and data quality monitoring provisions makes me want to look at the details of how, if at all, these requirements are being handled. Evidence of erratic demonstration and test results, often accompanied by ad hoc field changes, makes software deserve whatever bad things will be said of it. Poorly prepared or inadequate test materials and procedures for readiness tests and valid Logic and Accuracy tests indicate to me that shortcuts may have been taken elsewhere or that someone doubts the ability of the system to pass a meaningful test.

> Solution: Adherence to good practice in software design, coding, testing and documentation. Recognition of need for audit trails, security controls and performance assessment. Documentation of program description and operation, with supporting analysis such as flowcharts, HIPOs and data flowgraphs. Vendor-supplied module and system test procedures and acceptance criteria, and configuration and version control.

Administration: I do not profess expertise in the area of elections administration. I do look at how the administrative environment interacts with technical operations. It is common to find administrative regulations and procedures which deal ineffectively with the constraints necessarily placed upon things technical people do and how they must do them, and upon what degree of access to the process they may have. I look for posted procedures which define who is responsible for what, who has access to what, and who is accountable for what.

In particular, I am interested in who has the responsibility to conduct readiness tests and to determine the acceptability of test data. Next I want to know who will monitor equipment performance and personnel activities during the ballot handling and counting processes, who is responsible for detecting a problem and intervening when it arises, and what procedure must be followed to recover from it. I have seen correction and recovery procedures for some sophisticated central counting systems. I have never seen one for a precinct count system or for its centralized data collection and merging operations.

Finally, I am interested in the procedures for producing the official canvass of the election. The post-election activities which are necessary to rectify errors and include unprocessed and misdirected ballots are areas of major concern, and not just to the uninformed and troubled public. I wonder and worry too.

> Solution: Develop management, administrative and operational policies and procedures. Validate them in mock elections. Monitor and track adherence in live elections. Identify and correct deficiencies openly. Encourage the public to become informed, show their representatives how well you have done your homework, and do all you can to be responsive to the public's concerns.

Conclusion

If I have offended anyone by implying that there might be a bit of sloppiness here and there, I apologise. That was just to get your attention. There can be no real challenge to the way elections are handled in this country. Still, there is a lot of room for improvement.

My thoughts all come down to one point which has been stated or implied several times: "You must do your homework." You won't pass without it. A consultant can help you but his name won't be on the paper.

Here are some parting thoughts on what we can do to stay out of trouble, or to get out of trouble if our plans and prayers fail.

> Vendors should accept the responsibility of helping the user to acquire a system which meets the need, maybe a little more if that is cost-effective, but certainly nothing less. If you provide operational support, agressively assure that all aspects of the election are under somebody's control. If a deficiency is not your problem, make sure the user knows it exists, knows how to correct it and does so. Please, develop and validate recovery procedures for everything under the sun.
>
> Users should take overall responsibility for technical as well as administrative aspects. Make certain that someone verifies all operations, and that someone has signature responsibility for everything. Let the vendor be your strong right arm. Don't let anyone be your brain. Above all, try to anticipate every conceivable problem and develop contingency plans.
>
> Both should recognize that perception is just as important as reality, and that the election process can be demystified

by the active enrollment of the interested public. Think about how your plans will be perceived. Think about how your mistakes will be perceived. Try to make your world bulletproof. Do your homework. Keep all your papers to prove it. Continue to treat elections as matters of life or death. Politically, to all of us, they are.

THE CITIZEN AND POLITICAL SCIENTIST PERSPECTIVE

Richard G. Smolka
Professor, The American University and
Publisher, Election Administration Reports

Lance Hoffman gave me by far the easiest assignment for this conference - "The Citizen and Political Scientist Perspective." There are only about 250,000,000 citizens and perhaps 15,000 political scientists for whom I have been asked to speak. With that many out there, certainly a few will agree, at least in part, with what I am about to say.

The political scientist interest is straightforward. As a social scientist doing research, the political scientist wants certain data to be accurate and available. For the study of elections this data is frequently numbers - numbers of registered voters, numbers of voters who came to the polls, numbers of votes cast for each office and on each issue. In addition to numbers, information on ward or district boundaries is also necessary.

This information is usually sought not only for the immediate election but also for elections in recent years, and sometimes not so recent years. The history of registration, turnout and voting must be placed in context if results are to have meaning to the political scientist.

The way a political scientist and a candidate look at election results may be quite different. Candidates primarily want to know if they won, sometimes where they won and by how much, and often infer from the results why they won and what kind of mandate the election produced.

Political scientists also attempt to determine the answers to those questions but frequently look at broader issues such as "voter efficacy" - to what extent does a vote make a difference - and in broader terms, what a vote means to the voter who cast it.

Most political scientists rely on survey research rather than election returns for the answers to their questions. Such surveys attempt to identify the reasons why votes are cast for candidates, political parties and on issues.

Ideally, political scientists would like the ballots or ballot tapes given to them after the election is over because much could be determined by a closer analysis of individual ballots than can ever be learned from mere total votes cast for candidates.

There are conflicts, however, because winning candidates are not too happy to have the ballots examined closely at a later date. Suppose an error is discovered? Could there be a question about the legitimate outcome of an election? And what of ballot security while the political scientist has possession of the cards? Is it possible for the researcher, or someone else with access to the ballots during that period to add or substitute ballots to produce a different result and raise questions about the election?

Few winning candidates would favor any changes in election law that now provide that all ballots be held in secure custody of election officials for a specified period of time and then destroyed.

Those political scientists who want to work with election returns are often stymied because the best data is provided by individual ballots and these are often not available. When mechanical voting machines are used, there are no individual ballots to be examined, hence certain measurements, such as ticket-splitting, can only be inferred. Perhaps the individual ballot records retained by the new electronic voting machines can be made available to political scientists but some states by law may prevent this use.

Another example of political phenomena examined by political scientists is "voter dropoff," the phenomena of fewer votes being cast for offices as the voters moves down the ballot. We can determine, for example, how many voters came to the polls and how many cast a vote that counted for president and for other officers. Unless the ballots or ballot tapes are made available, we will never learn how many voted for president only, and skipped the remainder of the ballot. This type of information is easily available if paper ballots or punchcards are used.

Unless undervotes (fewer votes than permitted or no votes at all for an office) and overvotes (more votes than permitted) are reported, we will not know how many voters merely skipped a race or how many votes were invalidated because voters may have misunderstood the ballot and cast too many votes for the office.

Political scientists have also been asked to examine effects of such factors as method of voting, ballot layout, and districting and even type size and visibility of names and/or instructions on the ballot.

What concerns political scientists, therefore, is what kind of information and data is available, in what form, and when? Most political scientists are much more patient than candidates or politicians. Many work with election returns and related materials that are many years old. But the information and data must be available if they are to work with it.

Sometimes minor details about election reporting offend both candidates and political scientists. In most races computers are programmed to give the percentage of total votes each candidate receives. This makes sense when the voter is restricted to marking the ballot for only one candidate. But when the voter may vote for two or more candidates, the percentage of the total vote for an office makes little sense. The greater number of votes a voter is permitted to cast for an office, the worse the distortion caused by this reporting.

For example, if 100 voters go to the polls and 60 vote for the same three candidates for county commissioner, each candidate is reported receiving 20% of the total vote. Yet each candidate received 60% of the votes possible. The reporting would be clarified if the percentage shown were the percentage of ballots cast (100), not the percentage of votes cast for the office (300). Candidates, I am sure, would rather be reported receiving votes from 60% of the voters rather than merely 20% of the total vote.

The interests of the public may be less specific but no less demanding than those of political scientists. I would define the public in this exercise to include political groups, such as the League of Women Voters, voter watchdog organizations, political parties, voters and non-voters as well. Everyone must have confidence in the accuracy, integrity, and reliability, of the election process. The system must also enable all voters to cast their ballot in secret.

If the public is to have confidence in an election system, the system must work well for voters, candidates, parties, and the press. Voters must be able to find out where and when to register; to verify easily whether they are registered; to know where and when to vote; to know which candidates for whom they are eligible to vote; and they must be able to vote within a reasonable distance without a long wait at the polls.

Information about the election process should be easily available including how to vote on the voting machines or devices used in the jurisdiction. Results of past elections should be available in a form that is easily understood. Methods of resolving election contests should known prior to an election and all procedures should be conducted publicly to ensure confidence in the process.[1]

Persons more active in the election process, such as political party representatives and voter watchdog groups, should be able to observe preparations for the elections including tests of election software and zero tests on mechanical voting machines. Whatever pretests are prescribed and reasonable for a voting system should be explained and open to the press.

Several factors contribute to public confidence including past reputation for honest elections, openness of the process, and level of public information. We can also add speed of election returns. Speed, although important, is more relative to expectations than to numbers of hours.

If final election results are expected at 11:00 p.m. but produced at 7:30 a.m. the following day, explanations must be made or there might be suspicions that dark deeds occurred during the night. If however, it is anticipated that complete results will not be available until 1:00 a.m. and they are made available by 12:45 a.m., there is usually little criticism even though a more efficient procedure could have produced them by 10:00 p.m.

I can speak with authority on the subject of what the public wants and what it sometimes gets from firsthand experience in my own jurisdiction, the District of Columbia. When nearly half the ballots cast are invalidated, the public is outraged.

In 1976, the D. C. Board of Elections ruled invalid 40% of the ballots cast in the 1976 Democratic presidential primary election. Although much of the fault must go to the local Democratic party for its complicated ballot procedure, instructions to the voter left much to be desired. Ultimately half the invalidated ballots were ordered counted by the court. Yet, one in five voters who came to the polls did so in vain. Their votes were not counted.

People still talk about year precinct ballot boxes with voted ballots in them were placed in green plastic garbage bags to protect them from the rain. Some of these bags fell off the open trucks transporting them from the polls to the central counting location and were temporarily lost. Although all were recovered by the next morning, needless to say, this procedure did nothing to instill confidence in D.C. elections.

Other basic errors included obviously incorrect precinct vote totals for mayor and council. It took several days to correct these numbers while the outcome of certain races remained in doubt. One election the city used registration lists that failed to include thousands of validly registered citizens including the chairman of the city council, the publisher of the Washington Post, the Republican National Committeewoman who was herself a candidate for reelection to that position on the ballot, and other prominent officials and citizens. When they were told at the polls that they were not registered, it made national news.

The series of debacles triggered radical reform in the D.C. election system. Emmett Fremaux, the current director, recruited from New Orleans, has been recognized as administrator of an agency now cited as a model of efficiency in the city government.

I also believe that even simple changes in terminology can help public confidence in a system. In punchcard voting systems, ballot cards that cannot be processed by cardreaders are sometimes "duplicated" so that the vote can be counted automatically. The idea that a ballot is duplicated certainly arouses suspicion.

Why not call the card that enters the card reader a "ballot tally card" or almost anything else other than a "duplicated ballot." The person who creates the "ballot tally card" is actually recording the choices made on the ballot marked by the voter. Counting someone's ballot seems to me to be more acceptable than "duplicating" a ballot even though the process is identical.

As new voting systems are introduced, however, it will be very important to ensure widespread public information and public acceptance lest confidence be eroded. Regardless of the changes, voters must know what to expect and data currently available to political scientists must remain available.

Some administrators seem to rely almost exclusively on the press to inform the public. Despite excellent coverage in some jurisdictions, reliance entirely on the press can be risky. Administrators must accept responsibility for disseminating information directly to the voters. Whether this is done through direct mail, newspaper advertisements, and public service announcements, or other means appropriate to the jurisdiction matters little.

For the most part, the demands made by the public and political scientists on election administrators are reasonable and may even be useful. At worst, they may require a little more advance planning, a little greater public information effort, and perhaps a little more detailed election reporting but no radical changes. They may even facilitate turnout and help engender confidence in the political system.

Endnote

1. As a post-conference observation on the need for an open election system it may be noted that a federal judge in April, 1987, ordered a secret 25% manual recount of punchcard ballots cast in the March 3, St. Louis, Mo. aldermanic election. Incredibly, the judge ordered the recount for the Democratic nomination for president of the board of alderman conducted in strict secrecy under court supervision, subjecting all associated with the recount to contempt of court charges should they reveal any details of the recount. Later, the judge expanded the order to include a recount of all ballots, still keeping his gag order intact.

It is hard to imagine a recount procedure more likely to erode public confidence in the election system than one in which the basic information about it is kept secret from the public for months. As of August, 1987, the contest had not yet been resolved and the judge still maintained his veil of secrecy over the process.

A different factor central to the St. Louis controversy is directly related to the subject matter of this conference. The case now appears to be less a question of which candidate received the greater number of votes and more a question of whether punchcard voting per se discriminates against blacks.

It has been alleged that undervotes and overvotes for president of the board of alderman were greater in black precincts than in white precincts, and thus punchcard voting is discriminatory against blacks. If mechanical lever machines had been used, overvoting would be impossible, thus eliminating at least one possible "discriminatory" factor. It was once said, however, that lever machines discriminated against blacks when compared to paper ballots.

Resolution of the issue cannot depend upon analysis of a single variable. The impact of a voting system may be affected by the length and complexity of the ballot, the size of the printing, the height of the voter, the amount of voter information available, the length of time the system has been in use, the presence or absence of straight party options, rotation of names on the ballot, and many other factors.

According to a recent Iowa study, under certain conditions, undervoting is greater when mechanical lever machines are used than when punchcards are used. An Ohio study suggested that one system appeared to produce a greater proportion of valid votes for top offices but a lesser proportion for offices lower down the ballot. Should courts determine which is preferable?

Further, is it necessarily discriminatory if a greater proportion of voters of one race or one minority group choose not to vote for a particular office or offices in an election? Must undervotes always be an equal percentage? Whether some technical or mechanical aspects of voting systems have racial effects, and if so, what can be done about it, remains to be seen.

INTEGRITY, RELIABILITY AND SECURITY OF AUTOMATED ELECTIONS: A COMPUTER TECHNOLOGIST'S VIEW OF THE SCENE

Willis H. Ware
Senior Scientist, The Rand Corporation

Caveat: My a priori knowledge of the vote-counting industry is based solely on the group of papers furnished for the workshop, and on the personal experience of using such a system in Los Angeles County. I have also heard the discussion of the last hour here at the workshop.

A. Clarification of terminology. There are three properties which overlap to some extent. Sometimes a technical decision or action will support more than one of them.

- o Reliability -- a system does what it has been designed to do, consistently and without anomalous behavior.
- o Integrity -- a system is what it is expected to be; it has no surprises for the user. Thus, integrity is a component of reliability (although conceivably a system might have integrity, perform reliably, but not do the proper vote-counting job because of, say, a design glitch).
- o Security -- providing a system with an array of safeguards to protect it and its information against a defined threat. Such safeguards contribute to integrity but are not normally regarded as being specifically intended to counter the threat.

B. In the defense/foreign policy/intelligence world, the art of safeguarding information in computer systems is highly developed. A single Executive Order from the White House covers all of them and defines the terms "Confidential," "Secret," and "Top Secret" in terms of harm to the country if classified information is released to unauthorized individuals.

- o Good compusec can require safeguards in administrative and management controls, administrative and operational procedures, physical arrangements, personnel screening, communications, and technical computer hardware and software features.
- o The hardest of these is the hardware/software safeguards.

- o The others are generally easier to implement, are less expensive and collectively can afford a high measure of protection against significant aspects of the threat.

- o System design goes through a very formalized procedure.

  - Establish a threat statement.
  - Do a risk analysis.
  - Determine an appropriate set of safeguards.
  - Establish the cost of safeguards.
  - Iterate these last four steps as required, especially as unperceived vulnerabilities develop in the system through out its operational life.

C. The government has an established threat for defense intelligence.

- o It is the USSR and other foreign opponents--technically sophisticated, well-financed, and willing to buy information and/or subvert people.

- o It derives from centuries of experience in foreign policy, warfare, and intelligence activities.

D. For the commercial world, the threat is very different at present.

- o The current and dominant threat is the authorized insider who takes unauthorized actions, often exploiting his knowledge of the system, including the noncomputer parts.

- o Sophisticated technical threats are not presently important but are likely to become so as more security safeguards are installed and become effective.

E. What is the threat in computer-based vote-counting systems?

- o Is there even a threat? Is either of [C] or [D] the right one?

- o OR, is the problem the integrity of the system? Making it work properly, accurately, without anomalies, and in timely fashion.

- o OR, is the problem the reliability of the system?

- o OR, all of the above?

- o No one in the community, or even the community itself, seems to have a position on the first and basic step to system security, namely characterization and description of the threat.

F. In the vote-counting business, there are a large number of jurisdictions to deal with, each likely to have its own uniquenesses and laws. From a vendor's point of view, it is a market with diverse characteristics.

- o Election procedures vary widely and can be quite different. The structure of the ballot can vary from simple to utterly complex.
- o It is probably unreasonable to expect vote-counting authorities to have adequate knowledge on computer system security which is really a computer-related subject.
- o The odds are that jurisdictions are bimodally distributed. A large number of them are low in knowledge of computer security; and a few are wise in its art.
- o The documents and guidance from vendors seem pathetically sparse. Neither have the states or the FEC stepped up to bat.
- o The election community is largely unorganized.
- o There are no user groups organized around vendor equipment. Thus, there is little pressure on vendors to take desired actions.

G. Even if adequate doctrine, guidance, and detailed procedures become available from vendors and/or the FEC and/or the states and/or local governments, do the jurisdictions have the expertise and know-how to read and understand such material and translate it into appropriate action?

H. Except for a few large jurisdictions, the state of knowledge for system security, especially in software matters, in the vote-counting community appears to lie between very primitive and nonexistent. Likewise, the operational practices are not standardized; many jurisdictions probably invent their own.

- o This community is low on the learning curve of security.
- o It has not taken advantage of knowledge that exists elsewhere and is applicable.
- o It is not talking with the communities that are handling reliability, integrity, and security well

I. A lack of standards is antithetical to good computer system security.

- We cannot afford to have each entity doing its own thing; the job is too tough. There must be standards and uniformity.

- While electronic systems from the same vendor may appear to be the same in various jurisdictions, in fact they will differ in software details and almost certainly in operational procedures.

- Software variability as it now seemingly exists will make good system integrity and system security very difficult to achieve. Changes are reportedly made by programmers which implies actual changes in the programs themselves, probably not just adjusting parameters in the programs.

- There are well-known techniques for bringing software to a much higher state of standardization, yet with adequate flexibility.

- Limited local options are feasible but there should be a set of core safeguards that come with every system, including vendor (or FEC or state) supplied guidance on operational, administrative, physical, technical, and (if necessary) communications protections.

J. Summary: The election field,

- Has not developed the context for automated systems that has developed elsewhere;

- Does not have policy guidance from the Federal level or often from the State level;

- Does not have guidelines for even a minimum set of security standards and procedures;

- Seemingly does not have consistent terminology, especially with usage in other technical fields; and

- Is not exploiting knowledge already acquired and available in other fields of application of computer system technology.

K. The temptation from the user's point of view is to ping on the vendor, to point at him and complain; but....

- The world of commercial computer vendors (e.g., IBM, DEC) was not providing security standards and methodology either in the 1970s.

- It was afraid of offending the customer base by suggesting that the installed systems were vulnerable.

L. The election community cannot expect the vendors which support it to solve its security problem.

- It can and should expect vendors to supply systems that are reliable and have integrity.
- It can and should expect vendors to provide general guidance on security matters, especially training and awareness materials.

M. In the end, the election community must:

- Make its own decisions about threat;
- Make its own decisions about which safeguards to implement; and
- Be responsible for the secure performance of vote-counting systems and the integrity of the election count.

N. The NBS report (Pub 500-30) says it all re election security.

- The entire vote-counting community is low on the learning curve.
- Managements in vendors and in jurisdictions are especially so.
- It is a small market which means little motivation for a company of significant reputation and means to invest in it.
- Funding for doing anything is skimpy.
- There is lots of know-how and technology elsewhere that could be exploited to improve the situation.

O. If such circumstances still exist, it is going to be very hard to achieve a high level of system integrity and security.

- There is probably a Chernobyl or a TMI waiting to happen in some election, just as a Richter-8 earthquake is waiting to happen in California.

Appendix C. Tables of contents of current draft FEC standards

TABLE OF CONTENTS

Page

Page

Page

Appendix D. Findings and recommendations from the Saltman report

II. SUMMARY FINDINGS AND CONCLUSIONS

A. Analysis of Difficulties Experienced in Vote-Tallying

1. Findings

(a) Difficulties experienced in vote-tallying have included:

management failures, such as failures to institute adequate equipment and procedure testing and checkout,

human operational failures, such as errors in operation of computing equipment, and

technical failures, such as computer program errors and excessive punch-card jams in card readers.

(b) Failures of management have been responsible for most of the difficulties. Sudden technical failures, not predictable or capable of being considered in advance, have not been a significant factor.

2. Conclusions

(a) Better management procedures concerned with election preparation would have discovered most of the causal factors of subsequent difficulties and prevented the related technical and human operational failures.

(b) Technology and the management of technology are inextricably linked. The effective use of technology requires management control; and the effective management of technology requires the utilization of appropriate technological expertise.

B. Improving the Accuracy and Security of the Vote-Tallying Process

1. Findings

(a) Procedures that are widely practiced in many jurisdictions do not meet the high standards generally expected of the public election process. Among these procedures are those concerned with:

control and handling of ballots and other documents,

processing and reporting of vote-tallying information, operational control of computer programs and equipment,

design and documentation of computer programs,

control of the premises in which vote-tallying is done, and

management of the election preparation process.

(b) The assurance that steps are being taken by election officials to prevent unauthorized computer program alteration or other computer-related manipulations remains, nationwide, a continuing problem for the maintenance of public confidence in the election process.

(c) This study has not uncovered any facts which would serve to document any deliberate attempt to alter a vote-tallying computer program for the purpose of causing incorrect election results to be reported.

(d) The accuracy and security of vote-tallying is affected by factors outside of the vote-tallying system; for example, the voter registration process.

2. Conclusions

(a) The achievement of a level of confidence in the accuracy and security of a vote-tallying system which a government finds acceptable is dependent on the efforts and resources it applies. There is always a trade-off between resources expended and level of confidence.

(b) To maintain public confidence, information should be prepared and disseminated to voters indicating what steps are being taken by election administrators to assure the accuracy and security of the vote-tallying process.

(c) The problem of assuring correctness and security of vote-tallying computer programs is not significantly different than assuring correctness and security of computer programs used for sensitive financial and record-keeping purposes. Technical safeguards and management techniques developed for other applications can be adopted for vote-tallying programs.

(d) Active measures, beyond those now implemented in most jurisdictions are needed to protect the security and assure the accuracy of all aspects of vote-tallying. Among the measures that can be adopted are inclusion of audit trails and documentation in the process of program design and alteration, separation of duties in computer center operations, use of dedicated (non-multiprogrammed) computer operation, and physical controls over storage media containing sensitive application and support software.

(e) Specific measures can be implemented to aid in the audit of vote-tallying calculations. Among these measures are reporting of all undervotes and overvotes, ballot reconciliation and machine recounting on alternate, independently-managed systems.

(f) Specific measures can be implemented to effectively control ballots and computer hard-copy records for audit purposes. Among these measures are numbering of ballot stubs, machine-readability of each ballot's precinct number, and tight inventory control and documentation of the use of computer input and output media.

(g) Specific measures can be implemented to protect vote-tallying data during teleprocessing. Among these measures are synchronous transmission, the use of checksum polynomials, and encryption.

(h) A complete consideration of the accuracy and security of vote-tallying would need to involve all connecting systems, for example, a computer-based voter registration system.

C. Improving the Management of the Election Preparation Process

1. Findings

(a) Extensive and thorough preparation significantly increases the likelihood of a smoothly run election and helps insure against the loss of public confidence which may occur as a result of administrative difficulties.

(b) The election preparation process is a system development project requiring acquisition of components according to a tight schedule, integration of complex subsystems, definition of complete and unambiguous operational procedures, and training of a large part-time staff in the expectation that the completed election system will operate flawlessly the first time it is utilized.

(c) Many of the difficulties that have occurred in elections using computers have resulted from failures to appreciate the complexities of management of a development project with an absolutely fixed deadline and the special requirements necessary to insure successful operation of complex electronic equipment.

(d) Functional and physical specifications to which electronic and mechanical components must adhere, any acceptance testing of these components, and sufficient simulation, testing, and checkout of the election system and its most complex subsystems are strikingly lacking in a significant number of State and local jurisdictions.

(e) The ballot, the vote-encoding equipment, the voter, and the sensor of the ballot form a subsystem causing the voter's choices to enter the data processing part of vote-tallying. The correct operation of this subsystem is of paramount importance to overall system accuracy and to a smoothly-run election.

(f) A computer program for vote-tallying meant to run on a stored-program computer can be treated like a product on which design controls and acceptance-test criteria can be imposed.

2. Conclusions

(a) Successful concepts of project management that have been widely utilized in high technology industries such as electronics and aerospace can be adopted in the election preparation process.

(b) Concepts that can be adopted include critical-path-method scheduling, contingency planning including the availability of back-up equipment, development of functional and physical specifications and acceptance testing of vendor-supplied hardware and software, and extensive simulation and checkout of the specific configuration of the election system including all its subsystems.

(c) Acceptance testing should be separate and distinct from pre-election checkout. No hardware or software which is not of a model that has previously passed an acceptance test in conformance with design specifications should be permitted to be used in an election.

(d) Design and documentation requirements can be imposed on computer programs used for vote-tallying to improve their reliability, intelligibility, and capabilities for testing and auditing. Among the specifications that can be imposed are use of high-level language, use of table-driven code, use of modularity, inclusions of audit trails, specific provision for entry and exit of test data, flow charting and extensive use of comments among the program statements.

(e) Design specifications and acceptance testing of the ballot, vote-encoding equipment and the ballot sensor can be coordinated. These equipments can be given a combined acceptance test using a statistical sample of voters to simulate actual voting conditions. It can be determined in this manner if overall system accuracy and expected speed of operation can be achieved.

(f) The chief local election administrator should have full management control over all the resources (personnel, equipment, supplies and sites) that will be used in an election. His control should be maintained until voluntarily relinquished following completion of vote counting.

(g) Election administrators and vendors must agree beforehand on the specific responsibilities each is to assume during an election. A situation in which conflict of interest is a serious concern may be prevented if a vendor of election system components does not assume any responsibility for vote-tallying operations.

D. Institutional Factors Affecting Accuracy and Security

1. Findings

(a) In purchasing or leasing the products it uses, a single local jurisdiction is often forced by economic factors to choose among those products already in the marketplace. Imposition of special design criteria or acceptance requirements is difficult for a local jurisdiction because of its lack of market leverage.

(b) There is a lack of expertise in computer technology available within the structure of many local election administrations. In jurisdictions without technological expertise, vendors are more likely to conduct a significant part of the election on the administration's behalf.

(c) There is a lack of uniformity in the imposition of accuracy and security guidelines among local jurisdictions.

(d) There is a lack of precise technical terminology in regulations, leading to ambiguity in their interpretation.

(e) There is a lack of documentary information on the conduct of past elections, resulting in difficulty in precise determination of problems and difficulty in planning for improvements.

2. Conclusions

(a) Additional State leadership could alleviate the problem of lack of market leverage, and could satisfy the need for uniformity in accuracy and security guidelines and the need of local jurisdictions for increased technological expertise.

(b) Technological expertise within a State election administration can develop, on a Statewide basis, accuracy and security guidelines, design controls, acceptance tests, and definitions of technical terms; and can provide technical inputs to election policy decisions.

(c) Each State should insure that each of its local jurisdictions possesses the necessary expertise in computer technology to carry out its statutory election functions and does not rely primarily on vendors of election system components.

(d) The movement of ballots or electronic ballot images between counties or across State lines is an appropriate subject for State regulation due to the potential loss of security in that process.

(e) Local jurisdictions, following each election, should be required to file a report with the Chief State Elections Officer.

The report should include a summary by the local elections administrator of operational difficulties experienced and equipment malfunctions, and voluntary notarized statements by election participants attesting to personally-observed difficulties.

E. Additional Activities to Assure the Effective Use of Computing Technology

1. Findings

(a) At the present time there is no source of significant public funding for an organized program of research and development in the field of election equipment. In addition, administrative and technical failures of elections are widely publicized, and this fact may inhibit private investment.

(b) There is no consistent direction to election systems research, nor any concentration on those problems of research requiring large investments and long lead times.

(c) There is little, if any research being carried out systematically on the human engineering of voting systems. Therefore, no organized data are available on the effects of different kinds of voting systems and ballot arrangements on voting patterns and voting errors due to the human response to the equipment.

(d) Election administrators have a need to know the state-of-the-art of election technology, to insure that they will employ only proven technology that is reliable, well-engineered, and economical to use. They must know, also, some of the technological aspects of computer system operation and security and development project management.

(e) There is no organized technical information collection and exchange program among election administrators. With this situation, the exchange of experiences and solutions becomes an opportunistic and informal occurrence. This situation inhibits administrators from obtaining the data necessary for making the best choices in specifying, testing, purchasing, and operating elections equipment.

(f) Proposals have been made that results of computer-based elections receive an independent review and audit from an outside organization. The practicality of implementation of independent review and audit in every jurisdiction is questionable at this time.

2. Conclusions

(a) Coordinated and systematic research on election equipment and systems, independent of any immediate return on investment, is needed. Important areas requiring investigation are 1) the design of computer programs for greater intelligibility and ease of validation, 2) the human engineering of voting equipment, 3) the design of punch-card balloting equipment that locks out overvotes and improves chad elimination, 4) the design of new types of sensors and automated voter recognition equipment, and 5) designs of remote-access voting systems that improve voter convenience while preserving voter privacy.

(b) A continuing national program to collect and disseminate data among election administrators on election experiences and the state-of-the-art of new equipment and techniques would be valuable. Such a program would prevent redundant investigations and assist administrators in making the best use of scarce talent.

(c) Election administrators, in general, need additional training in computer security and computer operations, and in developmental project management to improve their capability to manage elections employing computing technology.

(d) A State that desires outside assistance in the development of additional technical capability within a State-level election administration should be able to obtain this aid through a non-proprietary arrangement that is designed to easily transfer this development experience to other States with low cost.

(e) The concept of election systems auditing needs investigation. The specific standards on which such an audit is to be based must be established and the auditor's specific duties with respect to an election must be delineated. The identity of the organization certifying the competence of the auditor needs to be determined.

(f) A National Election Systems Standards Laboratory would serve a valuable function for all States if established to set national minimum standards for Federal election procedures assuring accuracy and security, and similar standards for election equipment and systems performance. However, any Federal action to initiate such a laboratory should involve the cooperation and approval of the States to assure the laboratory's effectiveness.

Index