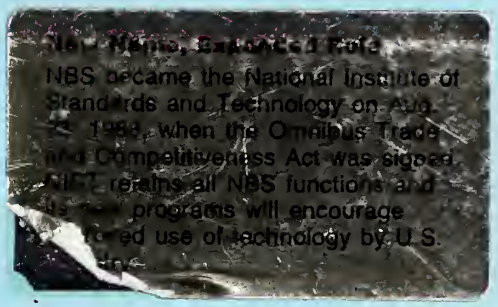
NBSIR 75-687

EFFECTIVE USE OF COMPUTING TECHNOLOGY IN VOTE-TALLYING

Roy G. Saltman

Information Technology Division
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D. C. 20234



March, 1975

Final Project Report

Prepared for
Clearinghouse on Election Administration
Office of Federal Elections
General Accounting Office
Washington, D. C. 20548

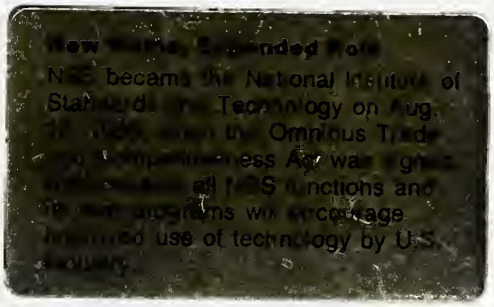
DEPARTMENT OF COMMERCE, Frederick B. Dent, Secretary
NAL BUREAU OF STANDARDS, Richard W. Roberts, Director

NBSIR 75–687

EFFECTIVE USE OF COMPUTING TECHNOLOGY IN VOTE-TALLYING

Roy G. Saltman

Information Technology Division
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D. C. 20234



March, 1975

Final Project Report

Prepared for
Clearinghouse on Election Administration
Office of Federal Elections
General Accounting Office
Washington, D. C. 20548

U. S. DEPARTMENT OF COMMERCE, Frederick B. Dent, Secretary
NATIONAL BUREAU OF STANDARDS, Richard W. Roberts, Director

ABSTRACT

The results of a systems analysis and evaluation conducted on the role of automatic digital processing in vote-tallying are presented. Included in the report are descriptions of hardware, software, and administrative problems encountered in fourteen elections in which electronic computing technology was utilized.

Methods of assuring more confidence in the accuracy and security of the vote-tallying process are presented and described. These methods include aids to audits of calculations, physical controls over ballots and computer records, and guidelines for the use of computer programs, computer facilities, and teleprocessing. Methods of improving the election preparation process also are presented and described. These involve the development and implementation of design specifications and acceptance tests for computer programs, election equipment and supplies, and guidelines for pre-election checkout of vote-tallying systems and for assurance of management control.

Institutional factors are discussed which should be considered if improved accuracy and security controls and more effective election preparations are to be implemented. Recommendations for additional research and other activities including a possible Federal role are provided.

Key words: Computer security; computing technology; election administration; public administration; state and local government; systems analysis; technology utilization; vote-tallying.

AVAILABILITY

This report is available from the National Technical Information Service, Springfield, VA 22161 under order number COM 75-11137.

In order to make the report more widely available, it was reprinted in 1978 as NBS Special Publication 500-30. This action enabled the assignment of a Library of Congress catalog card number, which is 78-5524.

ACKNOWLEDGEMENTS

The author acknowledges the contributions to this report by members of the professional staff of the Institute for Computer Sciences and Technology (ICST) of the National Bureau of Standards (NBS). These include Dr. Dennis Branstad, Mrs. Frances Holberton, Mr. John Little, Dr. Brian Lucas, Mr. William O'Toole, Dr. Selden Stewart, Dr. Rona Stillman, and Mr. William Truitt. In addition, helpful suggestions and reviews were provided by Mr. Edwin J. Istvan, Associate Director, and Michael Keplinger, Esq. of ICST, Dr. Patrick Eagan, Public Administration Fellow at ICST, and by Dr. Joan Rosenblatt and Dr. James Lechner of the Applied Mathematics Division of NBS. The author expresses his appreciation to Dr. Ruth Davis, Director of ICST, whose support enabled this project to be given the fullest possible attention.

Several State and local government elections and data processing officials gave of their time to personally meet with NBS representatives in connection with this project. These include Mr. Bernard Apol, Director of Elections and Mr. George Herstek, Jr. of the State of Michigan; Mr. Richard Banton, Assistant Secretary of State and Mr. Larry Bevens, Elections Coordinator of the State of Oregon; Mr. Norval Perkins, Executive Secretary to the Board of Elections and Ethics of the District of Columbia, and members of his staff; Mrs. Marie Garber, Elections Administrator, and Mr. Al Gruber of Montgomery County, Maryland; Mr. Leonard Panish, Registrar-Recorder, Mr. W. T. Kidwell, Chief, Data Processing, and members of their staffs of Los Angeles County, California; Mr. Robert Hamm, County Clerk, Mr. Kenneth Webb, Supervisor of Elections, Mr. Bob Nichols, Director of Data Processing, and members of their staffs of Ventura County, California; Mr. Jim Mayer, Acting Registrar of Voters, and members of his staff of Orange County, California; Mr. Herb Sammis, Registrar of Voters, Mr. Eldon Jones, Elections Supervisor, and members of the staff of Riverside County, California; Col. David Nicol, Director of Elections of Maricopa County, Arizona; Mr. John Weldon, Director of Elections of Multnomah County, Oregon; Mr. J. W. Stephens, Director of Data Processing of Fulton County, Georgia; and Mr. George Edwards of the City of Detroit, Michigan.

Additional information was supplied by the Office of the Secretary of State, State of Washington; the California Commission on Voting Machines and Vote-Tallying Devices; the Offices of the County Clerks of Harris and Travis Counties, Texas, and Genesee County, Michigan; and the Office of the Elections Administrator, Fulton County, Georgia.

Useful discussions were held with several computer professionals who had been concerned with election problems while serving with chapters of the Association for Computing Machinery. These included Ms. Mary Ann Chapman of Austin, Texas, Mr. Dahl A. Gerberick of Long Beach, California, and Dr. George Dodd of Detroit, Michigan.

Representatives of suppliers of election hardware, software, and services also gave of their time to meet with NBS personnel in connection

with this project. These include Mr. Herbert H. Isaacs of Arthur Young and Co., Los Angeles, California; Mr. David Dunbar, President, and members of his staff of Computer Election Systems, Berkeley, California; Mr. Don McClure, Manager of Administrative and Property Systems of Computer Sciences Corporation Orange County Center, Santa Ana, California; Mr. Henry Forrest, Senior Vice-President, and members of his staff of Control Data Corporation, Rockville, Md.; Mr. Harry Wilcock, Marketing Representative for Cubic Corporation Votronics Vote Counter, San Diego, California; Mr. David Fry, General Manager, and members of his staff of Diamond International Corporation Election Services Department, Los Angeles, California, Mr. Richard McKay, President, and Dr. A. E. Smedley, Vice-President of Frank Thornbur Co., Chicago; Mr. William Underwood, Jr., President, Mr. James Theodore, Sales Manager, Election Systems, and members of the staff of Gyrex Corporation, Santa Barbara, California; Mr. Saul Schach, President, Mr. N. P. Abramowitz, Vice-President, and members of the staff of InfoComp Corp., Moorestown, New Jersey; Mr. William Hunter, Manager of Local Government Market Development for Sperry Univac, Washington, D.C.; and Dr. James Farmer of Systems Research, Inc., Los Angeles, California.

Acknowledgement of the assistance which representatives of State and local government, the Association for Computing Machinery, and private industry provided should not be construed as necessarily implying their concurrence in the findings, conclusions or recommendations of this report.

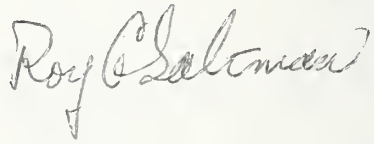


TABLE OF CONTENTS

FIGURES AND TABLES

I. BACKGROUND

This report has been prepared in fulfillment of an interagency agreement between the Institute for Computer Sciences and Technology of the National Bureau of Standards and the Clearinghouse on Election Administration. The Clearinghouse was, at the time of the agreement in February, 1974, a component of the Office of Federal Elections of the General Accounting Office and had been established under section 308(c) of the Federal Election Campaign Act of 1971. That section of the Act provided for the Clearinghouse to contract for independent studies of the administration of elections. The subjects of the studies, as provided in the law, could include voting and counting methods. As a result of legislation enacted in October, 1974, the Clearinghouse is to be merged into the new Federal Elections Commission; and the new legislation provides for essentially the same function that the Clearinghouse performed under the Federal Election Campaign Act.

The Institute for Computer Sciences and Technology was established to carry out the responsibilities mandated to the Department of Commerce by Public Law 89-306, "the Brooks Act", and its duties were further delineated in several Bureau of the Budget letters and by departmental order. Long-term objectives of the Institute's program which are pertinent to this report are to: manage the Federal Information Processing Standards (FIPS) program, provide advisory and consulting services in computer sciences and technology to Federal agencies, expedite the innovation and diffusion of automation technology in public services, and perform technological assessments of computer science and technology activities for the benefit of government.

In recognition of concerns expressed in Congress and by election officials and the public, the Clearinghouse, through the General Accounting Office, requested that the Institute study the use of computers in vote-tallying. Such concerns 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.

The Institute was specifically asked to "conduct a systems analysis and evaluation of the role of automatic digital processing equipment in the vote-tallying process."[1] Included in the analysis was to be an identification of the hardware, software, and administrative problems that had been encountered; an evaluation, where possible, of the causes of the problems; and an analysis of "methods currently being employed . . . to detect and prevent computer vote fraud."[2] Areas of investigation were to include election system design, training of election officials, ballot accountability, certification and inspection of computer programs, independent audits of election processes, counting center security provisions, and ballot recounts. The Institute also was specifically asked to "develop operational guidelines that election administrators could implement to help insure

the accuracy and security of the vote-tallying process."[3] In addition, the Institute was requested to assess the impact of new technological developments involving computers on the vote-counting process and to provide information on how those developments might be employed and made secure.

Of particular relevance to this study of the use of computers in vote-tallying is the Institute's program on computer security. Among the objectives of the computer security program are to provide methods of protecting personal and confidential data through the application of good information practices and to apply technological measures for controlling access to data in computer systems and networks. Some of the publications of the National Bureau of Standards that are concerned with computer security are referenced in this report.[4,5,6,7,8,9,97]

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 th t 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 sit tion in which conflict of interest is a serious concern may be prevented f a vendor of election system components does not assume any respo ibility 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.

III. CURRENT USE OF ELECTRONIC, PROGRAMMABLE VOTE-TALLYING DEVICES

A. Computer-Tallying of Punch-Card Ballots

The first significant use of punch-card ballots and computers to tally them was in Fulton and De Kalb Counties, Georgia, in the September, 1964, primary election. In the Presidential election of November, 1964, in addition to these two Georgia counties, the same type of system was employed in Lane County, Oregon, and San Joaquin and Monterey Counties, California.[10] The use of this form of voting has expanded considerably since that time, and at present, about 10% of American voters use punch-cards as a voting medium. More than 30 states have passed legislation permitting punch-card ballots. Of the 100 largest U.S. cities, 16 used punch-card voting in the 1972 general election.[11] Los Angeles County, the nation's most populous, uses the system, and in the 1972 presidential election, about 2.9 million voters used punch-cards in that County. The system is most pervasive in the western states, for example in California, Oregon, Arizona, and Hawaii.

The initial use of these systems typically was in conjunction with business computers that were being employed for a variety of applications by governments or nearby corporate installations. As the price/performance ratio of computer hardware has decreased, individual computing facilities used only for vote-tallying have become more economically feasible. This new trend towards minicomputers used only for vote-tallying and possibly other non-concurrent operations such as voter registration, is likely to continue.

The particular system initially employed in Fulton and De Kalb Counties and the most widespread system in use at this time was developed from a concept introduced by Dr. Joseph P. Harris, a political scientist and former government administrator. As the system is currently implemented, the voter is given a pre-scored punch-card of standard size, with a numbered stub attached, which he inserts in a mechanical holder. The card itself contains no voting information except that, in general, the pre-scored locations are uniquely numbered. One card format contains 235 voting locations. In most cases, only one card is needed by a voter to vote for all offices and issues.

The holder has attached to it a loose-leaf booklet which is centered over the inserted punch-card, exposing only one column of the punch-card to the view of the voter. As the loose-leaf pages are turned, a different column of the punch-card is exposed for each page. The voter must turn all pages to insure that he obtains all the pertinent voting instructions. The information visible on the pages includes the names of the offices and identifications of the issues to be voted, the names of the candidates and alternate responses to issues, and the maximum number of allowable votes for the office. The names of the candidates and issue responses are positioned on the pages so that each clearly corresponds to a different pre-scored location.

The voter, using a stylus, punches the pre-scored locations corresponding to the choices for which he desires to vote. The hand-held stylus punches out the "chad" from the card, creating holes. Following the voting process, the numbered stub is removed from the card while the voter's choices are protected by an envelope. The card is then collected with all other voted cards and delivered to a computing system.

A second type of voting device for punch-cards, developed somewhat later, also employs a standard-size card with an attached, numbered stub, but which is not pre-scored. In this system, the pertinent information is printed on the cards. The holder into which the card is inserted has fastened to it a hand-operated mechanical punch which can move up and down the length of the card and which is enabled for punching only at locations centered on allowable voting positions. In this system, the chad is removed by the punching die. Only one column on one side of the card is used, and the card often must be turned over and in many cases, additional cards employed to complete the voting for all offices and issues on the ballot. As with the first system described, these cards, after the stubs are removed, are collected and delivered to a computing system.

Pre-scored punch-cards have been used also for absentee ballots, even when a jurisdiction continues to use lever machines (mechanical "vote summarizers") in its local precincts. The absentee voter generally receives his card ballot on a styrofoam backing. The styrofoam provides a good surface against which to remove chad and also stiffens the ballot during mailing. Two jurisdictions that have used punch-cards only for absentee ballots are Detroit, Michigan, and Montgomery County, Maryland. In Montgomery, the candidate names were printed on the card next to the corresponding pre-scored location.

1. Functions of the Computer Program

Voted punch-card ballots, delivered to a computing system, are read by a card reader and the data thus sensed are transferred to a storage unit of the computer. Typically, cards from a single precinct are read in succession and are preceded in the reader by a header card which identifies the precinct. A specially-written computer program counts allowable votes from all punch-card ballots read. The program causes a computer-driven printer to print out the results for all offices and issues.

A fact of all voting systems currently in use that employ card or paper ballots of any type is that the voter cannot be physically prevented from overvoting, that is, voting for more candidates than can fill a particular office. Overvoting is identified by the computer program that processes the ballots. The program is usually arranged to eliminate any vote for an office that has been overvoted but count votes on the same ballot for other offices that have not been overvoted.

The design of the vote-tallying program must allow for variations, depending on the needs of the jurisdiction in which it will be used. Differing formats for presentation of results are common. In Oregon, overvotes and no votes must be shown to demonstrate a vote reconciliation, but a similar reconciliation is not required in almost all other jurisdictions. In Michigan, the card ballot includes straight-party ticket locations. If any one of these locations is punched, votes for all partisan candidates of the indicated party will be counted with the following exception. An otherwise allowable vote for a specific candidate of a different party will override a punch in a straight-party ticket location. This logic must be built into the vote-tallying computer program.

B. Mark-Sense Ballot Systems

In addition to punch-cards, other forms of machine-readable ballots and associated reading equipment are in use today in various jurisdictions, for example in Riverside and Orange Counties, California. These machine-readable ballots employ various kinds of markings made by the voter that can be sensed by reading equipment, hence the use of "mark-sense" in this report as a generic term applying to any of these systems. "Optical character recognition" is not employed generically because the frequency spectrum used for detection in some systems similar to the optical type is not in the visible range. Optical recognition, then, is simply a single type of mark-sensing. Recognition of the change in electrical conductivity due to a pencil mark is another type of mark-sensing.

For example, in one system, the voter uses a rubber stamp with fluorescent ink obtained from a stamp pad to mark his ballot in the appropriate locations. The sensor recognizes the fluorescence. In another system, a rubber stamp is also employed but the ink has a property of good infra-red reflectivity which is employed by the sensing equipment to read the ballot. In a third system, the voter employs a dark pencil and the sensing equipment, genuinely optical, distinguishes between light and dark. In still another system, a pencil mark is recognized in the infra-red spectrum. The shape of all ballots in these systems is typically rectangular although the dimensions of the sides are different in different systems. Except for one newly-introduced system, the dimensions are not the same as a standard data-processing card.

A similarity of mark-sense systems is that the facilities of general-purpose, commercially-available business computers usually cannot be employed for ballot counting without special modifications. Business computers typically include, as standard, reading equipment for punch cards or perforated tape but not mark-sense readers. However, in Multnomah County, Oregon, a specially-designed interface has been in use for several years, permitting a mark-sense reader to provide information (via teleprocessing) to a general-purpose computer; and an optical character recognition sensor attached to a general-purpose

computer was employed in the September, 1974 District of Columbia primary election. Minicomputers, supplied with special purpose software for vote-tallying and designed to receive mark-sense ballot data are feasible.

1. Ballot Summarizers

For most mark-sense voting systems, an essential component is a "ballot summarizer," a special-purpose computing device which receives the information on the ballots via the sensor and summarizes the number of votes separately for each voting location on the ballot. The ballot summarizer must eliminate overvotes while engaged in the counting process. The output of the ballot summarizer is typically the number of allowable votes recorded in each voting location on the ballots, the number of ballots which it read successfully, and the precinct and ballot style identification. (The ballot style is the unique set and sequence of candidates appearing on the ballot in one or several precincts.) This information issues from various machines in any of several forms: printed on paper, punched on paper tape, and/or punched into standard data processing cards. If the summary information for each precinct is obtained on punched cards or punched paper tape (or transmitted in digital electronic form) a general-purpose digital computer can then be employed without further transcription to complete the final processing for each office to be voted. Otherwise, typically, the precinct results on paper are summed manually or with desk calculators to generate the final answers.

A characteristic of typical ballot summarizers in order to permit them to be used in more than one election is that they are programmable to a limited degree. That is, it must be possible by design, after the device has left the factory, to specify to the device the number of candidates for each office, the number of allowable votes for each office, and the locations of acceptable marks on the ballot. The programming is carried out in various ways, depending on the design of the device. A punched card or punched paper tape containing instructions for the device may be inserted into it, and/or various dials and switches may be set. In one device, a plug-in programmable read-only memory (PROM) is used. In addition, the ballot summarizer must contain sufficient storage for at least as many candidates and issue responses as are on the ballot. To the extent that it is programmable, contains internal storage, and performs logic operations, the ballot summarizer is similar to its more general-purpose cousin, the stored-program computer.

As with the stored-program computers, there are ballot summarizers that are meant to be centrally-located, receiving ballots from many precincts; and there are those that are precinct-located.

C. Electronic Vote Summarizers

The State of Illinois, in March, 1974, approved for use in

that State a new type of electronic voting device which can be classed as an electronic "vote summarizer." The voter operates the device by pushing a set of buttons related to his choices. He finalizes his choices with a "complete" button, and thereby causes his votes to be added to the total votes previously recorded by the machine. The device summarizes the states of pushbuttons representing votes, not ballots, and so it cannot be classed as a ballot summarizer. However, similar to a ballot summarizer, it contains storage to record vote totals; and is programmed to accept votes which must be related to particular storage registers. It is programmed also to perform addition, to accept votes for more than one candidate when allowable and to reject overvotes.

The particular device approved in Illinois is programmed by internally-stored data introduced into the memory of the device on a magnetic tape. The vote totals from the summarizer, obtained after the polls are closed, are found on electronic digital data displays. Direct transmission of these results to a general-purpose computer is possible. Two counties in Illinois, Coles and Lee, tested the device in the November, 1974, general election.

IV. EXAMPLES OF REPORTED DIFFICULTIES EXPERIENCED IN VOTE-TALLYING

Of the many elections which have employed machine-readable ballots and/or computers to assist in determining the results, a few experienced major difficulties. In these elections, a tally from all precincts was delayed well beyond 24 hours after the polls closed, or serious allegations of fraud or sabotage were made, or the counts as released were later found to be substantially incorrect. In some other elections, difficulties were reported, but of less severity. In these, some delay or garbled output resulted, but the errors were soon corrected or a later speedup compensated for the earlier delay. Some of the various problems which have occurred are described below, but these descriptions must be read with the following cautions:

First, it is not intended that these descriptions be the complete and definitive versions of what occurred during these elections. Only brief abstracts of conditions are given.

Second, no definitive proof can be supplied that events occurred exactly as described. An election is a public event, not a laboratory experiment, and, unlike a laboratory experiment is not subject to verification by repetition under identical conditions.

Third, the information about events has been obtained from the reports of participants or observers in these elections, and therefore is based on their personal interpretations. Quotations from newspaper reports are given when these are the only readily-available sources of printed information. Strong efforts were made to report only those incidents that were noted by more than one source, and direct quotations are provided where appropriate. Editorial comments from the press are reported in order to demonstrate the depth of feelings and to underscore the importance which is ascribed to well-run elections.

A. Major Difficulties

1. San Francisco, November, 1968:

San Francisco used lever machines to summarize voters' choices at the polls in the election on November 5. The city then tried to have the grand totals compiled by having precinct workers transcribe the numbers on the lever machines on to sheets which were to be read into computers by optical scanners, but this procedure was a failure. The final results were compiled by adding machine.

The San Francisco Chronicle reported that "the initial problem was created by officials at polling places who neglected to enter the number of votes cast on the special sheets prepared for the computer."[12] Computerworld corroborated this with the statement by the city's chief administrative officer that most errors resulted from election workers transposing, changing or dropping digits when transferring numbers to the scanner sheets. "Many of our trained workers

pulled out at the last minute, so we had many persons working on election day who didn't have time for much training" , the administrator was quoted as saying.[13]

On November 18, it was reported that the San Francisco Grand Jury had called for an end to computer vote counting and a return to manual methods,[14] but the troubles were not over. On November 22 it was further reported that the official counts in two races were more than 12,000 votes different than originally reported.[15] The Chronicle later commented in an editorial "the discovery last week during the official election canvass that up to 13,000 votes cast on election day were not included in the unofficial election night returns is astonishing, alarming, preposterous and confidence shaking, but unfortunately not incredible."[16]

Coincidentally, a successful variation of the type of operation attempted in San Francisco in 1968 has recently been reported from Anne Arundel County, Maryland, in its September 10, 1974, State-wide primary.[17] In this case, conversion of the lever machine data was done at the central computer center as a result of phoned-in summaries from individual polling places. Tally sheets filled out by telephone answerers were passed to the data-entry supervisor. Four data-entry operators keyed the data to disc through a commercially available key-to-disc system and verified it. The disc data was dumped to tape after each set of 5 precincts' results had been collected, and the tapes were used to update candidates' totals held in the computer. The system produced complete unofficial results from 82 precincts 3 1/2 hours after the close of the polls. The official count, one week later showed no change.

The differences highlighting the Anne Arundel experience are that the critical data conversion operation was done by a small number of professional data-entry operators rather than a host of volunteers, and that only solidly-reliable technology was employed. The essential decisions implementing the form of the system were made by an experienced data processing manager.

2. Los Angeles, June, 1970:[18,19,20,21,22]

There were several types of difficulties experienced in this election, but the most serious concerned the misprinting or omission of some of the ballot-holder inserts that related a candidate's name to a particular hole in the ballot card. In one instance a candidate's name was placed out of correct rotational order in some ballot-holder inserts, resulting in an erroneous vote count for that office. In other instances, some of the insert pages were missing and thus some candidates were not listed. In some cases, it was not possible to reconstruct the vote by manual counting, since not all ballot-holder inserts in different voting booths were incorrect in a precinct. Since all the cards, when voted, were dropped in the same box, those voted in different booths could not be separated.

Other errors concerned the non-delivery of 40,000 sample ballots, failure to mail some notices advising citizens where to vote, wrong addresses for polling places and the mailing of one party's ballot for this primary to another party's members. Consolidation of local elections had resulted in an unexpectedly large ballot size, and there were extensive delays in printing, collating and mailing.

During processing of the ballots, some of the difficulties were as follows. Some precinct numbers were lacking on the voted ballots. This produced overwhelming work for the ballot inspection teams. Some header cards were missing or wrong header cards were present. Some header cards did not have control data as to the total number of votes and write-ins. An error was discovered in the tallying program when the logic and accuracy test was completed one hour after the polls closed. The error was corrected. Card reader operators were not well-trained; some cards were inserted in readers upside down. Six unscheduled core dumps occurred during ballot processing that were due to operator error. During one restart procedure after an unscheduled core dump, a programming error was discovered. The program was saving only 2,000 vote counting registers instead of the 2,700 specified. Twenty-three hours after the polls closed, it was discovered that votes from 540 precincts were missing. A search disclosed that votes from 492 of these precincts had been loaded on tapes which were found in a cardboard box in the computer room. The ballots from 48 precincts were found in the inspection area, unprocessed.

Approximately one-half of one percent of all ballots had failed to read in the card readers on initial processing. Observers noted that when the ballot inspectors would fan a two-inch deck of ballot cards after receiving them, clouds of chad (the small punched pieces of card) would fall out. Investigation of this phenomenon showed that it was due to the voters failing to completely remove the chad in the voting process. Many of the card reader jams were due to chad.

In addition, two computer tapes containing all the votes cast for 531 precincts were found to be physically defective and had to be remade from the ballots themselves. The ballots had to be removed from the safe where they were stored, and in order to have the necessary persons present when this was done, the process had to wait until the Friday after the election. Results were held in abeyance until then.

Following the election, the Los Angeles County Board of Supervisors created a Special Election Task Force to investigate the situation, and the task force hired Economics Research Associates to conduct a two-phase consulting effort. Results of that study are cited in Chapter V of this report.

An intensive effort was then put forth by Los Angeles County to insure the success of the November, 1970 election,[23] and this effort was fruitful. "Hard work, extreme care, and intense scrutiny to detail paid off--the election count ran as smooth as silk", it was reported.[24]

3. Fresno, June, 1970

The only difficulty in this election was that the computer program needed to count the punch-card ballots was not completed before the election. In fact, it was not completed until several days after the election and vote-counting could not begin until 87 hours after the polls closed. The Fresno County government had only one software specialist trained in the necessary computer language and that person was required, in addition to writing the vote-counting program, to assist in other-day-to-day data processing activities.

The possibility of a delay in the completion of the program was reported the day before the election. The Fresno Bee quoted the County's Auditor-Controller who supervised the county's data processing system as saying that a few "little problems" were discovered.[25] On election day, with the program still not completed, a team of programming experts from the computer hardware manufacturer's organization were called in to assist.[21] A major problem seemed to be the large number of different ballot formats, about 2,800.[26] It was admitted that the time required to complete the program was underestimated to a significant degree.[27,28] In an editorial after the completion of the vote-counting, commenting on a "So What? We Have a Little Delay" statement attributed to a member of the County's Board of Supervisors, the Fresno Bee said, "Each hour's delay in the vote tally added to Fresno County's position of humiliation in the nation."[29] The "So What?" comment was also reported by Datamation.[22,30]

The State of California later passed legislation requiring that a certified copy of the computer program be submitted to the State Commission on Voting Machines and Vote-Tallying Devices several days before an election.

4. Detroit, August, 1970

The primary election in Detroit on August 4, 1970, was the first use of punch-card voting in that city. Outside of Los Angeles, that election and the general election in Detroit in November, 1970, are among the very few elections using punch-cards that have been extensively documented. According to a report prepared for the Michigan Senate Standing Committee on Municipalities, violations of Michigan election laws were extensive, as were violations of the Interim Rules for Electronic Voting Systems issued by the Secretary of State of Michigan, July 8, 1970, and the Election Inspectors Instructions issued by the Detroit Elections Commission.[31] There was considerable confusion and a "great public outcry concerning the change to the computer-oriented method of voting, the preparation and conduct of the election, and the delay in the vote count."[32] Seventy-three hours elapsed from the time the polls closed until the final count was completed.

Six different regional computer counting centers using computers borrowed from private industry were initially established. It was planned that a tally of each precinct would be printed and punched

at the regional site to which a precinct's ballots were taken. Punched tally cards would be taken to a summary computer site at the City-County Building where unofficial city-wide tallies would be printed.

"Although six counting sites were provided for the August election, programming and procedural problems prevented all except one site from beginning operation on the night of the election. The availability of all the non-operational sites terminated the morning after the election. Although several of these sites became available again and were used for short periods, the initially operational site processed in excess of eighty percent of the ballots."[33]

The vendor of the computer program failed to provide the vote-tallying programs to the city election commission fourteen days before the election and provide a certificate of accuracy, as required by regulation.[34] However, an accuracy test was run seven days in advance.[35] The public accuracy test required to be conducted prior to election day on all the automatic tabulating equipment was only done at the City summary computer site and only 76 of the 1,111 ballot styles were tested. By law, the equipment at all sites and all ballot styles should have been tested.[36] When the same test was attempted using duplicated test decks at five of the six regional centers on election night just before the ballots were to be counted, the test failed. The results added one vote for just one candidate in every precinct. The other centers could not begin processing. George Edwards, the City Clerk, stated that "we spent three hours at least trying to correct the error in the program." After one site reported that an actual box of ballots ran perfectly, "we began to assume that the problem was in the test deck."[37] Unfortunately by the time the problem was solved, it was about six o'clock in the morning and three of the centers could not be used again because they were required to be returned to their owners or lessees, the private businesses from whom they had been borrowed. Furthermore, at two counting centers where the premises were owned by private businesses, the public was not permitted to observe operations, as required by Michigan election law.[38]

There were many procedural difficulties concerned with the setting up of polling booths, documentation of the voting, and the movement of ballots. There were deliveries of the voting devices to wrong buildings.[39] Examples of precinct chairmen not maintaining accurate records in the poll book and not balancing the number of ballot cards used against poll records were reported.[40] Failures to deliver ballot cards or failures to deliver ballot cards properly prepared were noted.[40] Transfer cases were not packed with the correct materials in many cases. "There were at least 10 or 12 precincts that went through check-in centers and ended up without any cards in them" said Mr. Edwards.[41] As of two days following the election, the location of one precinct's ballot cards was still in doubt.[42]

There were reports of defective equipment. "We may have had in some precincts...equipment which did not have the rubber strips at the base of the ballot card holder in such a position as to physically

catch and therefore fully remove the chad," according to George Edwards.[43] The Metropolitan Detroit Chapter of the Association for Computing Machinery, acting in a "public interest" capacity, reported:

"Design inadequacies of the voting device (the ballot holder) resulted in its failure to meet the close tolerances necessary to avoid punctures and hanging chad. Excess space between the porta-punch pad and the perforated template on some voting devices allowed the ballot card to buckle slightly within the device so that the template hole and the scored rectangles were not aligned....Lack of rigidity of the template and its thinness allowed the stylus to be inserted through the template at an acute angle and consequently to strike the ballot card off-center of the rectangle....

"Since the ballot labeling was always on the left side of the ballot card, it was natural for a left-handed voter to position his hand above rather than to the left of the ballot card. In this position, the temptation to angle the stylus is strong..."[44]

These design difficulties promoted extra punctures in the ballot cards and hanging chad. Violations of regulations were reported with respect to the removal of chad at check-in centers.

In tallying, "we had far too many card jams in the computer," said Edwards.[45] The average rate at which ballot cards were read was 45 cards per minute, although the expected rate was nearly 4 times that.[46] "Experience has shown us that the ballot cards used are too frail. First, they are susceptible to changes in the weather in that they absorb moisture and thereby cause computer jams. Secondly, we have found that when running a given precinct four, five, or six times through the computer there may be a tendency for one or more chads to 'pop out.' This, of course, would change the vote totals in that precinct."[47] If chad was caused by voters failing to fully disengage the chad while voting, this problem can be overcome by voter education and experience, according to Edwards.

Despite these difficulties which were widely reported in the national press,[48,49] the Detroit Common Council voted to try the same system in the November elections of that year. This election, also, was the victim of major problems, and afterwards, the City returned to its former method of voting. However, the City tried again with punch-card voting in the September and November, 1973 elections, tabulating only its absentee ballots on minicomputers rented especially for the occasion. These efforts proved successful, the 17,000 ballots in September and the 23,000 ballots in November being summarized in about four hours time each.[50]

5. Redford Township, Michigan, August, 1972

An error in the program used to count punch-card ballots in a primary election in Redford Township was not discovered until the counting was almost certified. The program had previously passed the

required logic and accuracy test without generating any suspicion of inaccuracy. Initial incorrect returns reported that a property tax proposition had been defeated by over 1,000 votes while in reality it had passed by just over 100 votes.[51]

The error was suspected by an election official who was suspicious that one unopposed candidate was getting several hundred more votes than another similarly unopposed candidate. Following a review of the program, the programmer admitted a logic error in a letter to a State official.[52] Two or three punches in a particular row were treated as inadmissible overvotes whereas in reality they were valid.

The logic and accuracy test provided for a different number of votes for each candidate or propositional alternative. The particular combinations that were incorrectly programmed had not been tested together.

The experience with the computer system in this election "has made me wonder how many other times it has happened around the country," the Township Clerk was quoted as saying. "How can you tell that it is not working when every test says it is running perfectly?"[51] Following the program change and the re-running of the program, the township hand-counted the ballots from one precinct to assure agreement with the computer results.

6. Harris County, Texas, November, 1972

In this first use of punch-card voting in Harris County, consternation and sharp disagreements resulted when a large number of ballots jammed in the card reader of the standard commercial computer used to tabulate them. Approximately 80,000 voters used punch-card ballots in this election, 40,000 at 39 precinct locations and 40,000 absentee. Although the incoming ballots were screened before they were fed into the card reader, the jamming of the ballots in the reader delayed results considerably. This delay was upsetting to local precinct officials who were forced to remain much longer than anticipated at the computer center to receive copies of their precinct results, as required by regulation.

The Houston Post reported on November 8, the day following the election that the Harris County Clerk "said it looked as if someone had deliberately tried to turn the county's first use of punch-card machines into a fiasco."[53] The story also reported that the County Clerk "said that as many as 15% of the ballots were mutilated by voters using ball point pens instead of the stylus provided in each of the booths. Although the cards could be read, each one had to be laboriously reproduced."[53]

In a phone conversation on September 12, 1974, an official in the office of the Harris County Clerk verified that the office still believed that there had been "deliberate misuse or abuse of the cards

themselves," and that the mutilation of the cards including holes in non-voting locations were done by ball point pens while the cards were not in the voting machines.

On November 10, 1972, the Houston Post reported again that the County Clerk's personnel were "convinced sabotage did occur,"[54] but on November 12, the Post reported a strong denial by a County political party chairwoman. "Claims made by the County Clerk that [political party members] organized a sabotage of the punch-card voting were 'inane', the chairwoman was quoted as saying, "the damaged cards and the foul-up in tabulating were the fault of election judges and the County Clerk's office..." "Clearly the whole handling of the punch-cards was a violation of the security and sanctity of voting rights,"[55] it was contended.

Although in the Post story on November 10, 1972, it was reported that a request had been made that "the Federal government should probe alleged sabotage and mutilation of punch card voting machine ballots during Tuesday's election in Commissioner's Precinct 3",[54] no such study (or any equivalent State investigation) was ever conducted. The charges made remained unverified and the situation simply passed into history.

In the primary election in May, 1974, Harris County used a minicomputer especially provided for election purposes, and in the words of an election official, "it was beautiful." The same type of system was planned for use in November, 1974.

7. District of Columbia, September, 1974

Difficulties that occurred in connection with the computerized ballot-counting system in the September 10, 1974, primary election caused the D.C. Board of Elections and Ethics to demand that the approximately 180,000 ballots (2 each from about 90,000 voters) be hand-counted. As a result, the outcome of the election was in doubt for about two weeks. The results of the hand-count "appear to support computer totals released nearly two weeks ago"[56] officials were quoted as saying on September 22, although the computer and hand counts differed in certain areas.

It became known election night and the following day that the computerized system was having difficulties and there were calls for investigations. Clifford Alexander, defeated primary candidate for mayor "called for the mayor [Walter Washington] to appoint immediately a commission or task force to determine what went wrong",[57] but "Washington turned aside the request."[58] City Council Vice Chairman Sterling Tucker said the Council would hold its own hearings. "We . . . want to find out how we all, including the board of elections, can avoid the kind of trauma we underwent last night,"[59] Tucker said.

A public hearing was held on October 3, after the vote count was certified, and it has been the only public hearing held on the September election as of February 1, 1975. At the hearing, only consultants and representatives of the D.C. Board of Elections and Ethics spoke. Representatives of the vendor of the vote-counting system, Control

Data Corporation, were present in the audience during the hearing but were not called on.

The views of the vendor and the D.C. government differ concerning difficulties that occurred in the operation of the vote-counting system. Press reports as a result of statements reportedly made by representatives of the D.C. Board of Elections and Ethics and the Division of Systems Development and Computer Services of the D.C. Office of Planning and Management represent one view. For example, it was reported that a member of the District's Board of Elections and Ethics "said the automatic counting was delayed because computers leased and operated by the Control Data Corporation were programmed incorrectly."[57] According to another report, Matthew Watson, counsel to the Board "blamed the computer snafus September 10 on the Control Data Corporation."[60] A report by the Division of Systems Development and Computer Services of the D.C. Office of Planning and Management was quoted as concluding that "the Control Data Corporation was responsible for the delays and foul-ups that eventually forced the city to recount all the ballots by hand."[61] The vendor, Control Data Corporation (CDC), has a different view.

Communication between the vendor and the D.C. Board of Elections and Ethics has been minimal since the election. Control Data Corporation requested a meeting with the Board following the election and the Board responded with a request that a written report be supplied first. CDC's view, according to their representatives, is that the situation demands a verbal explanation as well as a written report. Therefore, according to CDC, a meeting date should have been set, at which time a written report and verbal explanation would have been provided. As of February 1, 1975, no meeting between the Board and CDC substantively exploring the September election difficulties has occurred. CDC representatives did meet with the District's Material Management (contracting) Officer at which time a written report was submitted and a verbal explanation given. No Board members were present at that time.

The computing system used on September 10 included three CDC optical character recognition (OCR) scanners individually attached to three separate minicomputers. The minicomputers produced magnetic tapes of ballot images which were summarized on a CDC 1700 computer. Two CDC scanner-minicomputer systems had been employed in the May 7, 1974, District of Columbia Charter referendum; and in that election, the scanner output tapes were summarized on a computer system leased by the District from a different vendor. According to representatives of CDC, they operated the scanner systems on May 7, 1974, on a verbal agreement, assisting the D.C. Board of Elections on short notice when previous arrangements made by the Board fell through. The actual contracts for that election and for the September 10, 1974, primary election were not signed until July 29, 1974.[62]

For the September 10 election, CDC was to install a third scanner-minicomputer system and a CDC 1700 computer to process the tapes of ballot images. CDC representatives state that they had told the D.C. Board of Elections that unless a firm commitment could be obtained by June 10, 1974, no assurance of delivery and programming of the CDC 1700

could be made. The Board did not make that commitment until June 26, 1974, according to CDC[62] but CDC decided to proceed despite the earlier disclaimer. In addition, according to CDC, the necessary contract to permit modifications of the site for the CDC 1700 was never signed before the election, and CDC again proceeded in good faith in this area.[62] Failure to meet contract deadlines was one of the charges leveled against CDC.[61]

CDC was to supply the ballots for the election on September 10, but constant changes in ballot design prevented the actual ballots from being delivered until Sunday, September 8.[62] Changes in ballot design were ordered by the Board of Elections as late as August 28.[63] However, five hundred proof ballots were available on Friday, September 6 for the start of tests and checkout of the installed system. According to CDC, "on the morning of September 10, we were in a position of going on the air with a system, which because of indecisions on the part of the Board, could not be tested over a period of some time that would give us confidence in overall system operation."[62] Failure to fully test its equipment was another charge leveled against CDC.[61]

The CDC ballot design was very sensitive to the exact positions of the vote-mark rectangles on the ballot. In many mark-sense ballot designs, there are a fixed maximal set of locations from which the actual set of locations are chosen. Thus, in these systems, it is possible to partially test the system by inserting blank ballots which contain all possible usable locations in order to test system response to every location. With the CDC design, this type of pre-test was not possible. The exact locations with close tolerances were needed in order to test the scanner system.

Ballots were collected on election day at 10 a.m. and at 2 p.m., as well as at the close of polls at 8 p.m. Board of Election officials claim that one and perhaps two of the CDC scanners were not working properly at various times during the day. One scanner, according to a Board systems analyst, was down for about an hour during the morning of election day, and was taken out of operation completely about 2 a.m. CDC representatives deny that two scanners were not working but admit that one of the scanners was more sensitive than the others. This means that this scanner was "outstacking" more ballots than the other scanners. The scanners "outstack" (do not count) those ballots which they find to be blank or overvoted. These ballots are hand-counted. The more sensitive scanner was outstacking about 30% of its ballots, while the other scanners were outstacking 8-10%.

At 12:30 p.m. on election day, a CDC scanner operator was found to be making errors in operating one scanner in a manner that caused severe problems. The operator was supposed to flip a switch which inserted an "end-of-file" mark on the tape after each group of ballots from a single precinct. The operator was neglecting to do this, despite explicit instruction from CDC management. A decision had to be made. Either the ballots whose images were on the tape that had the missing end-of-file marks had to be run through the scanners again; or the program of the CDC 1700 had to be changed to permit that computer

to accept tapes without the end-of-file marks. It was decided to change the program of the CDC 1700.

Changing the program without a public test may violate the spirit if not the letter of the D.C. Rules and Regulations Title 22, Section 1.86 governing elections, which state that "a public test of the programs and equipment to count votes by machines shall be held within 4 days before the election . . . Notice of the test shall be given to candidates, party officials, the news media and to such other public representatives as the Board deems appropriate at least 7 days before the test."

Responsibility for making the decision to change the program of the CDC 1700 cannot be determined here. Representatives of CDC and the Board disagree on who actually made the decision. CDC states it merely responded with two technical and operational suggestions at that time: to re-run the ballot scanning and compilation process, or to re-program the 1700 computer. CDC states the subsequent decision was the Board's.

Representatives of the Board, on the other hand, have stated that no one at the Board of Elections was trained in the operation of the CDC 1700, and that CDC had responsibility for programming and operating the machine. It was the desire of CDC representatives to revise the program, they have stated, which they accepted.

The reason that the program-change decision was made rather than a re-scan decision may have been due to an attempt to minimize lost time. The need for timely reports of results to the media apparently affected many procedures for this election. One of the major complaints by the Board against CDC is that its 1700 machine, as programmed, was too slow and did not meet advertised speed parameters.[64] Observation of the speed of printing by the CDC 1700 showed it to be only one-half of what was claimed, according to the Board.

It was possible to change the program for the following reasons. First, the OCR scanners were reading the ballots' precinct identification numbers and could distinguish between different precincts by the fact that the precinct number had changed. Secondly, the tapes to be used by the scanners were supplied by the D.C. Government, and supposedly, the character "B" had been written at every character location along the tapes for the benefit of the back-up computer system which was to be operated by a separate vendor entirely. This action was taken on the morning of the election and CDC had only found out about it that morning. (A Board representative has stated that, although it is true that CDC had only found out about the "B's" that morning, the subject was discussed with two CDC systems analysts and according to the Board representative, they agreed the "B's" were needed.)

The writing of the "B's" had been done on an IBM 370 computer before the tapes were given to CDC. When the end of a scanner tape was reached by the CDC 1700, supposedly it could determine the end of the

tape by finding the first "B" that had not been over-written by ballot images. Problems with tapes were significant throughout the entire processing period.

First, many "B's" could not be found at the end of the tapes because of tape-head misalignment between computers. Unrecoverable parity errors resulted and tape operation was ended by manual intervention. Second, according to CDC, at least two tapes had defects in them which affected voting tabulations. The tapes were brand new and never previously used, a Board representative has stated, but they had not been examined for defects by the Board.

Third, a tape containing test data that could not be distinguished from live data was mixed in with the "fresh" tapes. This gave a tabulation which showed more votes in certain precincts (8, 49, and 62) than there were voters in those precincts. Fourth, tapes were being taken from the CDC area to the backup computer by Board of Elections personnel; and the tapes were being returned to the CDC 1700 after the backup computer was finished with them. CDC claims that one tape, containing morning-collection data from precincts 14, 73, 84, 85, and 91 was lost in transit by the Board of Elections and never returned for processing. In addition, claims CDC, a tape copied at the backup computer and then returned to CDC showed differences in ballot records for precinct 73 from the original of that tape. For precinct 74, 177 fewer ballots were counted in the first scanning than were counted in a later rerun, according to CDC.

Initial results from Ward 5, which included precincts 73 and 74, showed a very close race between two candidates, close enough to warrant a manual recount in any event. This manual recount showed significant discrepancies with the initially-computed results. As a result of the discrepancies, the full hand recount was ordered. By 6 p.m. on September 13, 70 hours after the close of polls, the complete computer output by precinct and ward with all errors corrected was available. It was this output with which the hand-count agreed two weeks later with differences noted in certain areas.

One additional difficulty is worthy of mention. When ballots of precincts 73 and 74 were being rerun on September 12 to check the original discrepancies, some additional ballots were "outstacked" over and above the ballots originally "outstacked." When ballots from these precincts were returned by CDC to Board of Elections personnel, the machine-counted ballots were returned to their locked storeroom, but the extra outstacked ballots were placed in a locked drawer of a Board of Elections systems analyst with his knowledge.[65]

CDC has reported that, according to their records, the number of ballots given to the systems analyst was 206.[62] However, the number of ballots reported by the Board of Elections and Ethics to be found in this drawer six days after the ballots were placed there was 91.[65] Board representatives accept 91 ballots as the number

originally placed in the drawer. This discrepancy remains to be explained.

On the basis of the facts as they are understood at this time, it can be concluded that problems of management, coordination, and division of responsibility among the various parties outweigh any actual technical failings in producing the serious difficulties that occurred in this election.

B. Minor Difficulties

1. Flint, Michigan, November, 1970

At the Genesee County data processing center, "difficulties were encountered in reading their 70,000 ballot cards,"[66] according to W. R. Penberthy, at that time Data Processing Administrator of the City of Flint. However, the final tabulation at the County's computer center was completed by 8:40 a.m., about 12 hours after the close of polls. The problem was in the card reader although there was not agreement as to the exact source of error.

Despite the belief of the computer manufacturer's customer engineer that the problem was one of humidity, the City of Flint's data processing system, located just five miles from the County's system, processed 58,000 cards without any difficulty at the same time. It finished its work by 6:00 a.m.

The story in Computerworld[67] that stated that forced drying and baking of ballot cards was tried in order to eliminate wetness was vigorously denied as "non-factual" by Mr. Penberthy in his letter to the Executive Editor of Computerworld.[66] Val Guerrier, Deputy City Clerk of Flint similarly stated on June 24, 1974, that the baking story was "entirely erroneous"[68] and that humidity was not likely the cause of the card reader problem since other locations did not experience any difficulty under the same weather conditions.

2. District of Columbia, January, 1971

Card ballots, printed by the District of Columbia government printer, jammed when run through card sorters used to count the ballots in this primary election to choose D.C.'s non-voting delegate to the U.S. House of Representatives.[69] J. E. Bindeman, chairman of the D.C. Board of Elections at that time was quoted as saying that the jams were due to variance in the width and texture of the cards. The District had printed the ballots itself in order to save money rather than order the cards from a large manufacturer.

Information from the D.C. Board of Elections and Ethics and from participating voters confirms that the statement in Computerworld[69] that "punched" card ballots were used was incorrect. The card ballots

were simply marked by the voters, not punched, and the card sorter was only used for counting, not sorting. A test run a week before the election had been satisfactory, but it was suggested that this was the case because the cards in the test were not actual ballots handled by the voters and election workers. On election night, one hundred students were used to count the ballots manually when it was clear that the automatic counting process was not working. The hand counting was completed early the next morning.

3. Los Angeles County, June, 1972 and November, 1972

The report "Computer Abuse" by Donn B. Parker, Susan Nycum, and S. Stephen Oüra, produced by Stanford Research Institute, November, 1973,[70] described this incident (quoted here in its entirety from page 110 of the report) as follows:

"7324N
"Vote Fraud, California--Vote Count Fraud.

"The county vote counting system produced identical vote counts in several precincts. Up to four precincts had identical vote counts. Fraud was suspected but no suspect found."

(The number 7324 is the report's identification number for this incident and "N means the case is not verified.")

According to Dr. S. Stephen Oüra, one of the report's authors, the basis of the description quoted above was a story in the Los Angeles Free Press of April 27, 1973,[71] entitled "Baxter Ward charges vote irregularity by computer" and an article in Computerworld on May 4, 1973, entitled "Accuracy of L.A. Vote System Challenged."[72]

The substance of the articles was that Mr. Baxter Ward, who had been elected to the Los Angeles County Board of Supervisors by winning the primary election of June, 1972, and the general election of November, 1972, had doubts about the accuracy of the Los Angeles County punch-card vote-tallying system. According to the Free Press article, "Ward said in at least 34 instances the precinct counts showed identical numbers of votes cast in successive precincts. He said in some cases the computer count showed identical vote totals for him in two precincts reported side by side. In some cases the votes were the same for three precincts and in at least one case the vote totals were identical for four precincts in a row."

Mr. Ward raised this question before the County Election Commission and asked for a thorough review, according to the Free Press story. A member of the County Election Commission was quoted as saying that "Mr. Ward makes some very serious charges which raise a question of honesty on the part of the county computer operators." The same Commissioner also said, according to the article, that Mr. Ward took the

June, 1972 primary material to the county grand jury but was turned down. It was unlikely, the Commissioner said, that the county computers had been fixed to favor some candidate over another. "Different results might be obtained but the number of collaborators required would make this improbable."

On November 6, 1974, a representative of the National Bureau of Standards discussed this specific situation with a spokesman for the Office of the Registrar-Recorder of Los Angeles County. The spokesman agreed that there were situations in which several precincts in sequence had reported exactly the same number of votes for one candidate (with differing quantities for the opponent), not only in the particular elections concerning Baxter Ward but in other elections and offices as well. This was not unusual, the spokesman said, because there were nearly 8,000 precincts in Los Angeles County and they were small, having roughly 400 to 500 voters each. In precincts that are adjacent, the populations are homogeneous, contain roughly the same number of voters, and similar voting patterns would be expected.

Furthermore, the spokesman continued, the Board of Elections had issued a specific recount order on this situation which had been carried out by the Registrar-Recorder's Office. The recount had been done on the November, 1972 ballots because ballots from the June, 1972 primary were no longer available at the time the Board of Elections requested the recount, the law requiring that ballots be retained for only six months. Fifteen precincts identified by Baxter Ward had been hand recounted with neutral observers present. These precincts included two "3-in-a-row" situations. In the thirty counts (fifteen for him and fifteen for his opponent), 28 showed identical totals to that reported by the computer. In one instance there had been a change from 173 to 174 votes for Mr. Ward, and in another case there was a change from 164 to 165 votes for his opponent.

In addition, the spokesman noted, the story in Computerworld[72] that stated that "there is now a manual recount of 20 precincts after each county election" is incorrect in that fact. The law requires a manual recount of 1% of the precincts, and since the county has nearly 8,000 precincts, at least 80 would have to be recounted. Actually, 100 are recounted. Twenty each are selected by the four political parties on the ballot in Los Angeles County and the remaining twenty are selected by the Registrar-Recorder.

No further action has been taken on this situation by either Mr. Ward or the Board of Elections, the spokesman added.

4. Travis County, Texas, November, 1972

Problems with jams of punched card-ballots in the card reader, and programming and operating system problems created some

difficulties in processing the election results in Travis County in November, 1972.

Certification of the ballot-counting program was attempted on the night before the election. In the course of this test, an error was discovered in the ballot-counting program and two instructions were added to it to correct this condition. Certification was then completed.[73]

On election night, processing was begun with a single-job executive system although certification had apparently been carried out using a multiprogramming executive.[74] Card jams began immediately, but these were able to be cleared for the first three precincts run. A card jam occurring in the fourth precinct was cleared but the program would not continue. The operating system would not return control and apparently was looping within itself.

In attempting to restart, the files on the three completed precincts were destroyed, so that these were loaded again with punched precinct summary cards. The first time the precinct summary cards were loaded, one card was found to be incorrect by the political party "watchers" and had to be re-punched. The cards were loaded again.

At that time, it was agreed to switch to the multiprogramming executive because of the looping problem and because certification had been carried out using it. With this executive, card reading speed was cut in half, but there were fewer card jams.

After processing an additional nineteen precincts, a decision was made to switch again to the single-job executive in order to increase card reader speed. This was done; and at the same time, the first three precincts were completely run again, so that their summaries would be in a permanent file. (When the summary cards had been loaded, these values did not appear in the permanent file, but only in a file which would be destroyed during a restart.)

When the first three precincts were entered again, after the switch to the single job executive, the count of one precinct did not match with the first run of that precinct. It was decided after some re-runs that a card jam the first time had caused the difference.[74]

One more looping problem occurred requiring a time-consuming restart. No other problems except card jams occurred and ballot processing was completed about 9:30 a.m.

"It is believed that the cause of the card jams was the reading of the card starting with column 80 entering the read station first. That edge of the card is a perforated edge [from] which the ballot stub had been torn..."[73] Reversing the ballot would have made a smooth edge registering at the card read station first. A program change, which could not be done election night, would have been required to allow the computer to accept the ballots in the reverse direction.

5. King County, Washington, September, 1973

The failure to insert a program control card resulted in some obviously erroneous election results that were initially reported. When the mistake was pointed out to the data processing organization it was corrected.[75,76] The failure to insert a header card also generated some incorrect results initially, as cards from two precincts that voted in the same location were mixed together. This error was also easily corrected after it had been made known.[76]

The following editorial comments from a Seattle newspaper on this election are not complaints about technical errors, but concern institutional questions which cannot be ignored:

"Election officials so far have failed to respond properly to the technological and human changes created by punch card voting.

"Use of the new computer election system has had its fallout. Not only has it been generally slower on election night to inform the public about what candidates are winning what race, but from a human standpoint punch card voting also has had an impact...

"Many [election day workers] report they do not like to work at the polls since it is now impossible with punch cards to keep track of the ballot results as reflected against the number of persons who have signed in to vote. In a sense, technology has displaced them as the watchdog of their party on the voting process."[77]

6. Washington Township, New Jersey, November, 1973

The first test of punch-card voting in this Gloucester County jurisdiction went smoothly excepting for a problem with the punch-cards employed. Each voter was required to use two cards, but the manufacturer had supplied the two types of cards in lengths that were one-sixteenth of an inch different.[78] The difference caused some mis-readings of the cards by the card reader, and this caused erroneous tallies that were noticed by alert watchers of the results.

The problem was diagnosed in about three hours and was solved by the separate processing of the two types of cards.

In this election, in which punch-card ballots were used for all absentee voting throughout Gloucester County, as well as for precincts in Washington Township, the processing of those ballots was not done in Gloucester County. The ballots, and some election officials and deputies, were taken by bus across Camden County to Moorestown, Burlington County, to the offices of the vendor of the vote-tallying program. There, the ballots were processed on a machine leased by that vendor from a computer manufacturer.

7. Clackamas County, Oregon, May, 1974

In submitting disc space requirements to the operating system of the computer in preparation for this primary election, data processing technicians underestimated. Consequently, before all ballots had been read into the machine, all the space was used up. In order to continue processing, the totals were noted, the machine was cleared, and the remainder of the votes were counted. After unofficial totals were released, the disc requirements were increased and the entire set of ballots was rerun, this time in one continuous operation. The totals on the second time around matched those on the first two runs.[79,80]

V. ACCURACY AND SECURITY OF VOTE-TALLYING OPERATIONS

A. The Los Angeles Controversy of 1969

The issue of the security of computerized vote-tallying was publicly raised in Los Angeles in June of 1969 by several computer experts. They reported that there were methods with which computer programs used for vote-tallying could be secretly altered to rig an election. Although the potential alteration of computer programs is only one of many aspects of security in vote-tallying, it will be seen from the following discussion that the 1969 controversy touched on many related ramifications besides program alteration.

The computer experts involved in the specific situation in Los Angeles in 1969 did not claim that any particular election had been rigged (they had no evidence of that and only raised the possibility). Nevertheless, their report caused a considerable stir among politically-involved individuals in the Los Angeles area. It resulted in a page-one story in the Los Angeles Times on July 8, 1969, by political writer Richard Bergholz which described their conclusions and commented extensively;[81] and a television appearance by the Registrar-Recorder of Los Angeles County to deny the possibility of vote-rigging by means of the computer program.

However, the Board of Supervisors of Los Angeles County, taking the computer-experts' report as a challenge to the honesty of the conduct of County elections, ordered that a five-member committee on voting procedures be created to "investigate charges of computer rigging of elections." The City of Los Angeles asked that its own ballot-counting procedures be included in the investigation. The formation of the Los Angeles County Election Security Committee was reported nationwide: for example, in the New York Times on July 13, 1969,[82] and the Washington Post on July 24, 1969,[83] and both stories concentrated on the specific possibilities raised by the computer experts that programs could be secretly rigged. The possibility of rigging by this means has been raised repeatedly. For example, an article in Harper's magazine,[84] in November, 1972, quoted from Los Angeles news stories of 1969 and described the possibility of fraud without qualifying the statements with the conditions under which this could occur. The Los Angeles Free Press story of April 27, 1973, previously quoted, also editorializes without further explanation that "it has long been suspected that computers can be jiggered and fixed to give one candidate a better ballot count than another."[71]

The assurance that steps are being taken by election officials to prevent computer program alteration remains, nationwide, a continuing problem for the maintenance of public confidence in the election process.

The Elections Security Committee, chaired by Mr. Charles F. Horne, reported on March 3, 1970, that "no evidence came to the attention of the Committee to indicate that fraud has been attempted or perpetrated with the "system" in the County." The Committee also reported that

"qualified experts have testified that while computer rigging is technically possible, the chances of it are extremely remote... Election fraud by computer rigging would not be possible without collusion and deliberate intent among several persons having access to election computer and programs."[85]

The specific ways in which the computer experts, led by Dr. James Farmer, had said that vote-tallying programs could be rigged, were detailed in an article by Farmer, Springer, and Strumwasser in Datamation, in May, 1970.[86] They said that an extra bias routine could be added to the vote-counting program that would have certain characteristics to make it undetectable by the official "logic and accuracy" test. This routine could be arranged so as not to go into effect until a larger number of ballots had been counted than were in the logic and accuracy test sample; or could be prevented from being operative during the test and be activated by a computer operator only for the official count.

The fraudulent routine, said the article, could be added into the operating system, into the vote-counting program while it was still in source language, or into the vote-counting program after it had been converted into object code. To add the fraudulent routine into the operating system would, of course, require access to the system and the ability to replace it or modify it. The fraudulent routine could remain dormant until activated by a computer operator using a console switch, the article stated. Adding the bias routine into the object code would require either access to the object deck itself or access to the object code in the computer through the operating system. Rigging the count program in source code, again, would require access to it, but if such access could be obtained, the biasing routine would be of a simple nature.

The article recognized that a potential method for detecting fraud would be a check for changes in the lengths (numbers of instructions and data values) of the source code, object code, and operating system. But, it stated:

"Code added to a problem program would normally not be identified at the completion of development. A few instructions, without comment, could probably escape detection and, if noticed, not be identified. Since listings frequently have object deck changes or source changes on them, little concern would be evidenced over "minor corrections." In contrast to the layman's view, most systems are modified frequently to accommodate new conditions.

"Making changes in the object deck can be a trivial matter. Although operating systems normally identify replacement code or REP cards by listing them out, replacing cards and adding code is not difficult. If core sizes are controlled--and few audits include such sizes--then space can be found by replacing some unused or unnecessary function, some constants or shortening a code. Any programmer accustomed to reducing the size of programs--particularly for the early, small computers--can find space.

"Since programs are frequently the product of several people, the operating system is accessible to many, and object decks pass through many hands, it would be difficult to assign legal responsibility for a routine should fraud be discovered."[87]

The above quotation simply details loose practices, and the article, thereby, makes a point that cannot be denied: loose practices in the computer room, such as allowing uncontrolled access to sensitive programs, not documenting all changes to programs, not controlling access to the operations console, and not documenting all operating activities, can lead to serious loss of confidence in the computed results. When tight practices, including separation of responsibilities, documentation of all program changes and audit trails for all important computer room activities are in effect, the Election Security Committee's conclusion that "election fraud by computer rigging would not be possible without collusion ... among several persons having access..." similarly cannot be denied.

B. Los Angeles-Based Recommendations of 1969 and 1970

Recommendations for improving the controls over vote-counting by computer were made by Farmer and his associates in their Datamation article as well as by the Los Angeles Elections Security Committee in their March 1970 report. In addition, a second article in Datamation by Robert L. Patrick and Aubrey Dahl[88] made similar recommendations. Following the June 1970 primary election, Los Angeles County (through its Special Elections Task Force) hired Economics Research Associates (ERA) to analyze problems which occurred in that election; and after the November 1970 general election, the County employed Isaacs Associates, Inc. to perform an audit of the system used at that time. Both these firms made recommendations[18,89,90,91] concerning the security of the computer and its programs. In addition, a study of the Los Angeles vote-tallying system through March 1970 was prepared for the California State Commission on Voting Machines and Vote Tabulating Devices by Walter V. Sterling, Inc.[92] The recommendations made by all these firms although specifically developed with emphasis on Los Angeles, are generally applicable to any vote-counting computer system. Some of these recommendations have been instituted in many jurisdictions; and they have had a strong influence on the development of the guidelines provided with this report. Some of the more pertinent recommendations are as follows:

1. Audit Trails of Computations

Security Committee: "Require that computer programs be written to show total votes including over-votes, the number of over-votes, and the resulting net valid votes to make auditing and recounting more efficient and effective."

Patrick and Dahl: "Unbroken audit trails must be provided so that full accountability and auditability are provided. Penny accounting techniques should be used to treat each vote as if it is precious. Batch [precinct] totals must be provided, preserved, and carried through the system."

ERA: "Perform random program checks during operation. A dummy precinct could be used for this purpose and its totals checked to pre-calculated numbers."

Isaacs: "Improvements should be made to the existing computer programs to provide for more program checking and control of potential data errors, including the incorporation of explicit audit trails during operations."

Sterling: "A means should be provided to record the number of all 'no votes,' 'under votes,' and 'over votes.'"

2. Access Limitations

Farmer et al: "Strict access limitation during actual count procedures sufficient to assign responsibility to one person for any error."

ERA: "Tighten the security requirements for access to the main computer room. Physical security of the main computer room is an important factor in insuring the integrity of election night processing."

3. Observer Teams

Security Committee: "Observer teams composed of outside computer experts and other appropriate personnel [should] be established to observe data preparation, check-in center operations and all phases of the tally center operation."

Patrick and Dahl: "As a design concept, the programs and procedures should be open to scrutiny so that ignorance does not breed a charge of tampering."

ERA: "Ensure that [political observers] are properly briefed and consulted."

Sterling: "A system to provide election observers with system familiarization and procedural instructions" should be initiated.

4. Recounting

Farmer et al: "A redundant mechanical count should be made on a significant sample. The sample size should be selected to make the probability of undetected fraud low."

Security Committee: "A statistical recount of a random sample of ballots [should] be conducted after each election using manual, mechanical or electronic devices not used for the specific election."

Patrick and Dahl: "Provisions must be made to allow for partial recounts by precinct for each office/proposition."

ERA: "Implement a random recount procedure."

Sterling: "The percent recount required for each race or issue would be determined by selecting the tolerable level of an incorrect outcome, ... knowing the number of votes cast in the race, and the difference in the votes cast for the candidates."

5. Design of Computer Programs

Farmer et al: "Careful adherence to professionally accepted standards for programs [and] their documentation..."

Patrick and Dahl: "The computer programs should be designed clearly with tables defining ballot configurations."

ERA: "Use high-level programming languages where possible."

Isaacs: "...computer assistance in defining the multitude of different ballot styles for different voting districts" ... "computer programs that are [less] highly dependent upon operator interactions at the computer console."

Sterling: "It is recommended that a higher level machine language ... be used, and that comment statements be liberally utilized. Proper documentation, both written descriptions and flow charts, should be prepared... [the operating system] should be reduced to the minimum required operations necessary to properly execute the count/tally program."

6. Testing of Computer Programs

Farmer et al: "Development of a logic and accuracy test which uses the full range of election ballots, and which would, during execution, detect any unused code and list all counted program loops."

Security Committee: "Consider requiring an independent audit of the vote tally programs to reduce chances of program error or fraud."

ERA: "Perform a complete audit of the existing vote-counting programs."

Sterling: "A software audit is a necessary safeguard in preventing software fraud"... "All of the hardware and software used in the central processing, from initial ballot reading to the output of the official election canvass, must be included in and subjected to the Logic and Accuracy Tests."

7. Security of Computer Programs and Systems

Farmer et al: "Provision ... for in-process core dumps and

file duplication ... Requirements of ... program size control totals and all final compilations and tests retained (particularly from core dumps and loader maps)."

Security Committee: "Secure the operating system and the application programs as one unit. Lock out unwarranted actions on the console and log all actions. Generate an operating system that does not include multi-programming capabilities. Physically lock out all unused input-output devices. Physically protect the master console after initial program loading."

Patrick and Dahl: "Machine room procedures must be established to make sure no remotes are connected, to provide a clean visible workflow..."

ERA: "Implement program change control procedures... Physically protect the master console with a plexiglas cover."

Isaacs: "A post-election comparison of header cards used with the original ones produced [is] recommended."

Sterling: "Console operator commands should be limited"... "Single-person access to programs" should be prevented. "The 'double lock' security precaution should be applied to all forms of software that can be modified."

8. System Management

Isaacs: "Additional [local government] personnel should be made available to improve and maintain the election programs, to improve overall system documentation and training of new personnel, and to minimize dependence on outside contractors with unique program knowledge."

9. State Regulation

Sterling: "A study is needed to evaluate the State Election Code for clarity of the election criteria, consistency in applying the criteria to all methods of vote-counting, and adequate provisions for their implementation."

C. Vote-Tallying as an Operational System

A full consideration of the problems of assuring accuracy and security in vote-tallying must view vote-tallying as an operational system. Then, each element of the system can be analyzed for its protective requirements and every element can be seen as part of an integrated whole. There is little point in protecting one component and assuring its effective operation when other components are subject to gross deficiencies of control. It is important to begin with a definition of a vote-tallying system so that all of its parts can be identified.

One definition of "system" is "an organized collection of men, machines, and methods required to accomplish a set of specific functions." In this definition, a system is seen as having a specific output towards which the resources are working. In the specific situation which is the subject of this report, the output of a vote-tallying system is taken to be "the determination of the results of elections." If a vote-tallying system were seen as one which results in "voters registering their votes on ballots or machines" or one which results in "ballots having been counted" the recommendations of this report would have been necessarily different.

This concern with the definition of the system being considered is not simply semantic hairsplitting. If the concern is only with voters registering their votes, then in a punch-card system, the computer and its program are outside the boundaries of the system. Thus, any guidelines or mechanisms of assurance that concern the balloting process need not consider the computer; and there may be incompatibilities. Some of the difficulties which have been reported in the processing of punch-card ballots have been due to insufficient compatibility of the ballot as punched by a voter with the requirements of the automatic card reader for reading it. The interface between the ballot and the automated processing system (the sensing element) is fundamentally important to the accuracy of the election results.

Instead of defining the vote-tallying system as one that "determines the results of elections," it might be defined as a system that "counts ballots." This type of distinction has actually been made in Orange County, California, in order to permit that County's data processing vendor to receive individual precinct summaries in the form of punched cards and to compute their totals while not receiving the actual mark-sense ballots. According to a ruling of that County's counsel, for the vendor to receive the actual ballots and count them would be against the State regulations, but the receipt of precinct summaries would not.[93] The vendor is not seen as part of the "ballot counting system" in that County.

Thus, semantic distinctions about system boundaries have important consequences in administration and methods of operation, and these consequences effect decisions made about insuring accuracy and security.

A block flow diagram of a typical vote-tallying system using punch card ballots is shown in Figure 1. A boundary drawn around the system assists in the visualization of information flow into and out of the system. System integrity can be maintained only if information flow across the boundary can be limited in quantity and controlled in quality; and the maintenance of system integrity is a necessary condition for accuracy, reliability, and insurance against fraud.

The primary output of the system, as shown in Figure 1 is the "results of elections," although the system also provides the registration system with the names of those voters who exercised their franchise.

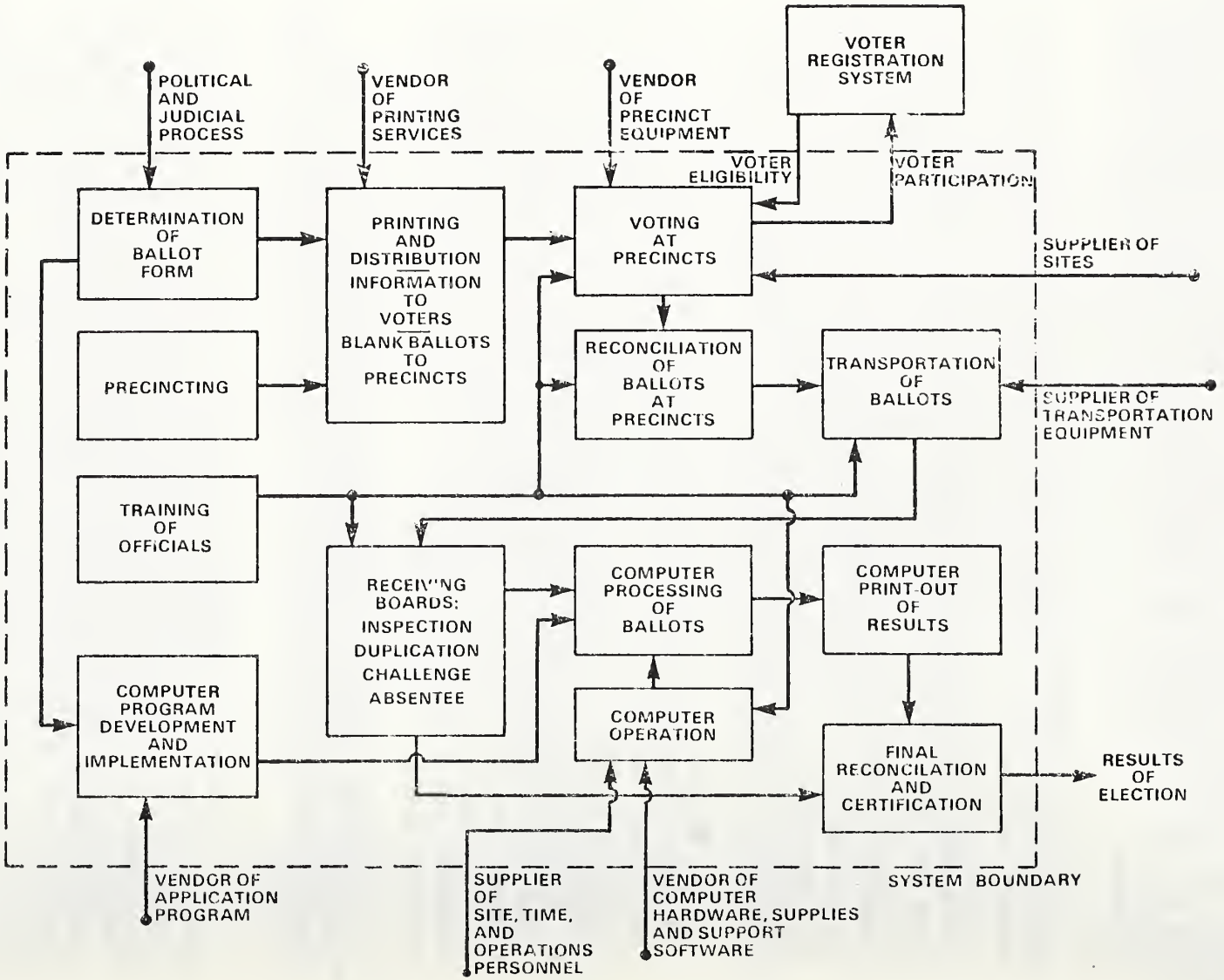


FIG. 1. EXAMPLE OF A COMPUTER-BASED VOTE-TALLYING SYSTEM

A primary input to which the vote-tallying system must respond is the political and possibly judicial process which generates the candidates and issues to be voted. The election system cannot control the quantity of this input, but hopefully through regulations, it can control its required "response time" to last-minute changes in this input necessitating revisions in the ballot. Since the definition of the ballot is one of the first steps in defining the operational vote-tallying system, the time at which it is finalized affects the time available for the performance of several other major vote-tallying tasks. If no specific time limitation can be imposed beyond which no change in ballot can occur, or if the last day for finalization allows insufficient preparation for the planned vote-tallying system, then detailed contingency plans must be held in readiness to allow for this situation.

An equally-important input to the vote-tallying system is the list of registrants permitted to vote. Attention to the vote-tallying system will be valueless if fraud is possible through a faulty registration system or the misuse of registration data.

There are other inputs to the system across its boundary, primarily provided by vendors of some of the goods and services used in it; but internal security, i.e., the management and control of the resources normally within the system by definition, must not be ignored. It is well recognized in the financial community, for example, that some of the most difficult breaches of security to detect and deter originate with those who understand how the system works because they are part of it.

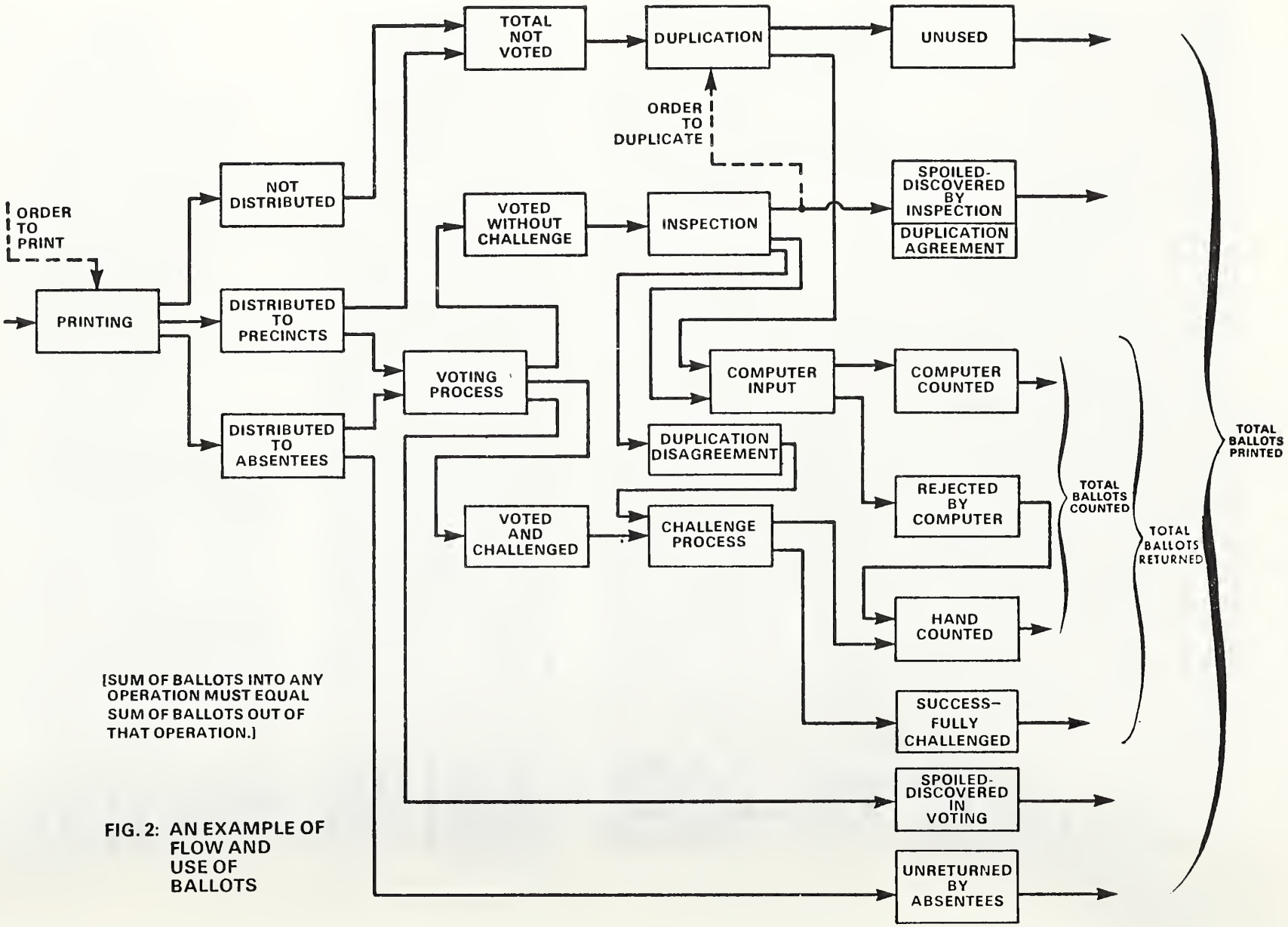
In reviewing the procedures necessary for assuring the accuracy and security of a vote-tallying system, a useful point of departure is the final block in Figure 1, "Final Reconciliation and Certification." At this point, the senior election official must make the ultimate decision to accept or reject the results provided to him. He must have supporting documentation that supplies the basis for his decision, and he must be certain that the rules under which the election was conducted leave no reasonable doubt as to the validity of the results. The following discussion describes and justifies some of the documentation that can be provided and rules that can be implemented.

D. Aids to Audit of Calculations

1. Ballot Reconciliation

An important aspect of the supporting documentation is data demonstrating ballot reconciliation. This implies a numerical balance between the number of ballots printed and distributed to precincts and the sum of all uses to which they were put. Figure 2 demonstrates the flow of ballots in a typical, but not necessarily universal type of election. The following is a description of this typical ballot flow.

First, the order to print is given and the number of ballots



[SUM OF BALLOTS INTO ANY OPERATION MUST EQUAL SUM OF BALLOTS OUT OF THAT OPERATION.]

FIG. 2: AN EXAMPLE OF FLOW AND USE OF BALLOTS

actually printed must equal the number ordered. Control documentation is needed at this point. Of all those printed, most are distributed to precincts and absentees and the remainder are sent to central headquarters for possible later use. Control documentation is needed for each precinct's receipts.

At each precinct, the ballots are either voted unchallenged, voted challenged, spoiled, or unused. Ballots are returned to central headquarters where two reconciliations for each precinct can be made. First, the number of voted ballots (of each individual type, in case each voter is issued more than one type), challenged and unchallenged, must equal the number of voters recorded as having been issued ballots. Second, the number of ballots received at the precinct must equal the number returned from the precinct in all categories.

The number of absentee ballots issued and the number returned must be noted for future reconciliations before the returned absentee ballots are dispersed into various counting categories.

All unchallenged voted ballots are then inspected for machine-readability before being machine counted. Chad removal from punch-card ballots, according to pre-determined regulation, occurs at this point. Some ballots are approved for computer (or summarizer) input as is, and the remainder need to be duplicated. Disagreement at this point as to exactly how a ballot should be duplicated sends the ballot to the challenge process.

In the duplication process, the originals are added to the "spoiled" total. The new duplicates are subtracted from the "unused" total and added to the total available for machine-counting. Control documentation is needed in the duplication process. Of those available for machine-counting, the machine actually counts most, and rejects the remainder. The latter are hand-counted.

In the challenge process, some ballots are successfully challenged and put aside and those permitted to be voted are hand-counted.

At the completion of counting, more reconciliations are possible. For each precinct, the number of ballots counted must equal (for each ballot type) the sum of the number machine-counted and hand-counted. In addition, for each precinct, the number of ballots issued must equal the number machine-counted, hand-counted, and not voted due to a successful challenge. Note that these reconciliations count ballots, not votes. That is, a blank ballot is still a ballot even if it is blank. Blank ballots must be counted for any ballot reconciliation. Furthermore, the total order given for ballot printing must equal the number remaining unused plus the sum of those used in all categories: machine-counted, hand-counted, successfully challenged, spoiled, and unreturned from absentees.

2. Vote Reconciliation with Undervotes and Overvotes

For those ballots that are machine-counted, an additional reconciliation is simple to accomplish and provides added confidence to the machine-counted results.

For an office in which the voter may vote for only one candidate, a ballot can contain only three mutually-exclusive results: (1) a single vote for a candidate, (2) an overvote, (3) an undervote (no vote). Clearly, the sum of candidate votes, overvotes, and undervotes equals the sum of the number of ballots voted for the office. To produce the reconciliation, the computing device must have storage locations for the number of ballots counted, the number of overvotes and the number of no votes. This reconciliation should be shown on the official precinct report for certification purposes, but need not be provided on election night.

A similar reconciliation for machine-counted ballots can be provided when the voter may vote for more than one candidate, say "N" candidates. To obtain a reconciliation in this case, the computing device must always assign N votes for each non-overvoted ballot counted. Up to N votes are assigned to the candidates selected by the voter, and the numerical difference, if any, between N and the number of candidate votes is added to the undervote storage location. If the ballot is overvoted for that office, a "one" is added to the overvote storage location for the office.

Then, the total number of candidate votes plus the total number of undervotes for the office equals N times the number of non-overvoted ballots for that office. The number of non-overvoted ballots is simply the total number of ballots counted minus the number of over-voted ballots for the office. One integer multiplication by N is required to be performed by the computing device in order to demonstrate the equality.

3. Verification of District-Wide Summations

When precinct totals are summed to produce district-wide totals, it is valuable to show a partial summation for each candidate's votes following the addition of each individual precinct total. The procedure of showing continuously increasing totals permits easier manual verification of the additions. The only other method for verification available is a check on the computer program itself.

Examples where failure to check long sums resulted in fraud have been reported.[94,95] A supermarket checkout clerk, by failing to close the cash drawer completely caused the cash register to retain the amount of the last customer's purchase in its summary register. The clerk was aware that the following customer had a very large order. The new customer received a checkout tape with every item correctly copied, but

the total reported by the cash register was incorrect. It was higher by the amount of the previous customer's purchase. The checkout clerk pocketed the extra money provided by the second customer. The checkout clerk reasoned that the second customer would not take the trouble to add a large number of items to check the total.

The extra printing involved in generating partial sums in an election report is valuable for presentation of official results, not for the release of unofficial election-night totals.

4. Recounting

The advantage of a hard-copy, machine-readable ballot is that an independent verification of the count is possible. Ballots can be recounted on a different machine or they can be recounted by hand. Machine recounting permits a larger recount with considerably less effort.

If a backup machine is available, and that is recommended as a good management practice, the ballots may be recounted on that machine. Further confidence in the recount may be expected if the management of the backup machine is independent of the organization managing the primary machine. An independent organization could be considered to be one that reports to a different elected official and receives an independent budget.

The current regulations covering recounts in different states vary. Some typical recount regulations are: (1) a manual recount can be demanded by any candidate and he pays for it, (2) a full manual recount is automatic if the candidates differ by a very small percentage of the vote, or (3) a fixed percentage of the precincts are manually recounted regardless of the vote-separation of the candidates.

A mathematical analysis of the confidence that can be obtained from different percentage recounts is presented in Appendix B. The analysis demonstrates that for a given level of confidence in the results, more ballots should be recounted as the opposing candidate vote totals become more equal. Numerical recount percentages are provided in the Appendix as a function of confidence level demanded, but as the candidate vote totals approach equality, the recount percentage for any confidence level approaches 100%.

The discussion of Appendix B shows that if only 1% of precincts are recounted, (the rule in California) and there are just two opposing candidates who differ by only 1% of the total vote, there is only a two-thirds probability with a recount of finding a type of worst-case error that might be overturning the outcome in an election involving 1,000 precincts. For there to be a 99% chance of finding this worst-case error when the candidates differ by 1% of the total vote, 4.3% of the precincts should be recounted, assuming a 1,000-precinct situation.

Therefore, to permit larger recounts, it is recommended that

rules be adopted which require mandatory machine recounts on a backup machine, preferably one independently managed. Furthermore, the recount percentages should increase as the opposing vote totals approach equality. If there is concern that running ballots through a machine a second time will alter the information contained on them, then there should be concern about the viability of that ballot system to begin with. Small sample manual recounts in addition to the larger machine recounts will further check the reliability of the results.

The selection of some precincts for recounting should be granted to candidates. As the analysis of Appendix B notes, worst-case errors occur when they are small enough to be beneath the level that would make them obvious by inspection of the apparent results. The candidates' supporters and precinct workers are those persons most likely to have the keenest sense that a possible discrepancy exists. Expected outcomes predicted by neutral political analysts that are very different than apparent outcomes should provide further keys to recount-precinct selection.

E. Effective Control of Ballots and Computer Records

1. Numbering of Ballot Stubs

An effective procedure to insure that control over the number of ballots issued is maintained so that ballot reconciliation can be performed is for each ballot to have a uniquely numbered stub. Even more effective control can be maintained if each ballot has two stubs numbered identically.

The ballots can be easily distributed to precincts in groups of about 100 if the second stubs of each group are stapled together to a backing. Ventura County, California, is one jurisdiction using this system. As each voter receives his ballot, he receives the ballot with the first stub still attached to the ballot. The second stub remains stapled to the backing. When the voter completes the voting process, the first stub is torn off before the ballot is dropped into ballot box or fed into a local-precinct ballot summarizer if that is the system being used. As the first stub is torn off, its number is compared against the number of the second stub which was retained when the voter received his ballot. These two numbers must agree or the voter should not be permitted to vote.

In addition to aiding ballot reconciliation, as two sets of stubs are available to precinct officials, the stubbing process helps prevent chain voting. In chain voting, one voter, instead of leaving his ballot at the polls, takes his unvoted ballot outside where it is marked by a person waiting there. That pre-marked ballot is then carried inside by a second voter who votes it. The second voter takes the blank ballot that he was issued at the polls outside where it is again marked for the benefit of still another voter, etc. Clearly, this process is

more applicable to a system employing a small ballot easily hidden on a person that can be hand-marked with a pencil or by pushing out pre-scored card locations than a large ballot not easily hidden or one requiring a special marking machine or special ink not readily available. In chain voting, the first voter loses his vote, but all succeeding participating voters vote as directed. Matching of the numbers of the two stubs prevents this illegal operation. In any event, whether a voter is participating in chain voting or not, he should be prevented from removing his ballot from the polling place. A voter should be able to obtain a second ballot, subject to regulation, if he spoils the first one he is issued.

2. Ballot Box Stuffing

Adding extra voted ballots into the counting system that were not voted by registered voters who actually appeared at the polling station is called ballot box stuffing. Its success is dependent on collusion or extreme negligence by election officials. Ballot box stuffing cannot be prevented by any security procedures established for the vote-tallying system alone. Its prevention depends on maintenance of accurate voter registration lists, and easy access by concerned citizens to the lists of those persons claimed to have voted. Access to lists of voters who voted will increase the likelihood that the name of someone not actually present for any reason will be recognized.

3. Machine-Readability of Ballot's Precinct Number

An important method of insuring that ballot and vote reconciliation activities can be correctly effected is for each ballot to be physically identified as to precinct. At present, ballots are often printed in manually-readable form with the precinct number or just the ballot style. The latter only identifies that group of precincts using an identical ballot. The precinct number (actual number or unique code identification) should be punched into the ballot or printed in machine-readable form if mark-sense equipment is being used.

Machine-readability of the precinct number assists in the prevention of ballots from one precinct being mixed with or exchanged with ballots of another precinct. The computing device must be programmed to read the precinct number and check it, if the identification is to have any value. This check is extremely important if ballot rotation is employed or if counting of ballots of more than one precinct is done at the same physical location.

If ballots from one precinct are mixed with or exchanged with ballots of another precinct, and the precincts have different sets of candidates in some races, incorrect results will be reported. Even if the precincts in which ballots are exchanged have exactly the same sets of candidates, but they are in a different rotational order, incorrect results will be reported. If an equal number of ballots are exchanged between precincts, the mistake would not be discovered by a ballot count reconciliation since the correct number of ballots would be found in each precinct.

The programmed check of the ballots' precinct number also reduces the importance of correct computer operator action in inserting a header card or other control card or tape that tells the computing device to which precinct the ballots belong. At present, a typical method of operation is for the computing device operator to insert a "header" card or tape that identifies the ballots which follow the header as coming from a specific precinct. This procedure provides the operator with an opportunity to commit an error that could generate incorrect results. If the ballots are precinct-identified and a programmed check is made, the precinct number need not be supplied by the header.

4. Control of Header Cards and Tapes

All header cards or other punched cards and tapes which program any computing device used for vote-tallying should be subjected to security procedures in their handling. The purposes of the security procedures are to be able to provide documentation for all election activities, and to specifically insure that the correct control materials are being used.

The blank stock from which the control cards or tapes are obtained should be controlled in quantity and should be visually distinct. Strict inventory control should be maintained when the control materials are obtained from stock for punching, and identification numbers should be placed on them. Retention and storage requirements applied to computer programs should be similarly applied to these materials.

5. Output Listing of Header Materials

Header cards and other program control materials used in the course of vote-tallying should be listed unmodified on the computer output printer as a means of verifying their exact content.

6. Verification of Candidate Rotation

Candidates should be listed on the computer output printer report for each precinct in the same sequence as they were listed on the voting instructions in that precinct. This action will further assure observers of the results that the computing device is correctly assigning ballot punchings or markings to the correct candidates, i.e. assuring correct rotation.

7. Control of Computer Output Hard-Copy

Cards that are punched as partial results of election totals should be treated as documentary evidence and handled accordingly. They should be obtained from blank stock that is controlled in quantity, visually distinct and numerically identified. The purposes of these controls are to prevent substitution of incorrect results and to document all relevant activities concerned with the elections. Computer output printer paper, when used for election purposes, should be similarly treated.

F. Security of Computer Programs and Systems

1. Typical Arrangements Today

In a typical situation existing today, a local election administration contracts directly with a vendor to obtain (for use on election night) an object deck of a vote-tallying applications program. The local administration submits its candidate and issue configuration requirements for the particular election to the vendor, whose plant may be located in a different State. The vendor specializes his general-purpose program for the particular election and returns an object deck (on cards, disc, or tape) to his local representative. The local vendor's representative, in conjunction with a data processing facility contracted for by the local elections administration, but not necessarily under the control of the elections administration, then tests the program and runs it on election night. The program is generally leased and therefore remains the vendor's property. The local election administration may receive a print-out of the program, but the print out may be in object code and therefore unintelligible to a human without insuperable labor.

Under these institutional conditions as described above, only a limited set of accuracy and security precautions can be taken. Additional assurances of accuracy and security require changes in methods of operation and in institutional relationships, and these are covered in Chapters VI and VII. Accuracy and security of the vote-tallying operations are intimately associated with the management of the election preparation process. Operations on election night, to insure accuracy and security, cannot be separated from the steps leading up to those operations. Chapter VI considers the question of testing the programs and other vendor-supplied items as "products" requiring design specifications and product acceptance tests. It also considers the question of system check-out in anticipation of election night operations. Chapter VII considers the problem of what institutional arrangements are necessary to enforce design specifications and product acceptance testing when local election administrations are small and lack both technical expertise and market impact.

The following paragraphs describe security precautions that can be implemented at the local level primarily assuming today's typical conditions given above.

2. Use of Dedicated Operation

The "operating system" of a computer is the computer's own supervisory program. The term "operating system" came into use when supervisory programs became sufficiently complex to permit more than one application program to be executed concurrently on the computer or to be executed sequentially without manual intervention.

The simplest operating system is one dedicated to a single task. At the next level of complexity, the operating system allows a

sequence of application programs to be run in succession. At a higher level of complexity, the operating system permits several application programs to run concurrently (multiprogramming). In this mode, several application programs may share the main memory of the computer at one time, and the operating system determines which one is executing at any one instant.

Further complexity is added by interactive operation. In this mode, a user maintains control of an executing application program by communicating with the operating system through the use of an on-line terminal.

At each successive level of complexity, the risk to security is greater. The operating system's job must include the activity of protecting application programs against invasions from each other, either accidental or deliberate, and must protect itself. Specifically, the threat is that if a penetration of an application program occurs, that program is subject to unauthorized alteration without the user's knowledge. Similarly, if the operating system is penetrated, all application programs that it controls are subject to unauthorized alteration. The essential problems of computer accuracy and security are to insure that first, application programs as written are exactly what the user intends, and second, that no unauthorized alteration occurs. The discussion of this section concerns the second item only.

Complex operating systems, at the current state-of-the-art, are never fully debugged and may contain many routines that could fall prey to tampering. Currently, no operating system with multiprogramming capability can withstand efforts of a determined penetrator to defeat the operating system's measures to prevent unauthorized alteration. If a general interactive capability is provided, the threat is greater as the penetrator is provided a measure of feedback as to how his attempts are proceeding.

It is concluded, therefore, that in order to eliminate as many security threats as possible, the least complex operating system that provides the capabilities required by the vote-tallying program should be used to support the vote-counting process. The computer system that executes vote-tallying programs, either for test or actual running operation, should be performing no other tasks at the same time. A system dedicated to vote-tallying both in testing and running, while vote-tallying operations are being performed, is preferred and highly desirable.

An excellent discussion of the problems faced in the security of operating systems is Chapter 6 of the Systems Review Manual on Security published by the American Federation of Information Processing Societies (AFIPS).[96]

Before beginning vote-tallying operations on a computer that has been used for other work, all extraneous peripheral equipment should be physically disconnected. The erasure of all memory locations that

are to remain accessible to the system except those minimally required to load a new operating system, if any, should be accomplished. Active measures must be undertaken to assure that all tapes and discs to be used that are supposed to be initially blank are actually blank (except for machine-readable inventory identifiers) and have no defects.

3. Use of Dedicated Support Software

The fact that a computer, when running vote-tallying operations does not run any other work, does not imply that the computer or its operating system may not be used at other times to run other applications. Thus, at these other times, the operating system or its support programs may be compromised or penetrated to later affect the operation of the vote-tallying program.

Therefore, separate copies of all computer support software such as the operating system, compiler, link editor, loader, and other needed utility programs should be obtained directly from a general supplier from his stock of standard products; or should be written in-house. Some assurance from a supplier that the copies received are standard products, unaltered in any way, is desirable. Listings should be received and stored for future comparisons. When these programs are obtained, the principle of least complexity needed, as described in the last subsection, should be adopted. Any routine, including those mentioned above, which operates upon any part of the vote-tallying program (even those simple routines used to copy files) should be maintained separately under the control of the election administration and not used for any other purpose except in connection with vote-tallying. Then, in addition, if the computer on which these programs are run does not perform any other work while executing any vote-tallying testing or running function, system security control at least can be isolated from outside computing influences.

4. Protection of Object Codes

A primary procedure for preventing unauthorized alteration in object codes is for master copies to be retained in secured locations, often physically separate from the location of working copies. Before use of the working copy, it is compared, bit for bit, against the master copy. Any differences must be explainable. Listings can be compared to insure that key instructions are still in the same physical and relative locations. The master copy, once generated, is always used in a read-only mode. No writing is ever done on to the storage medium of the master copy. This procedure can apply to all support software as well as to the vote-tallying applications program. When running an election, a reasonable procedure is to require a bit-for-bit comparison of all software used against master copies immediately before and immediately after ballot counting. When this bit-for-bit comparison is done, the computer should be under the sole control of the most elementary kind of supervisory program whose logic is obvious by inspection and whose sole function is this comparison. If it is ever necessary to generate

a working copy from a master copy, or to regenerate a master copy, a similar elementary supervisory program should be employed.

Other methods of protection include assuring that key instructions remain in their known relative locations and that the number of instructions remains fixed. If the object code can be altered, it can be provided with a routine which will prevent its further execution unless certain key parameters known only to a few people are inserted on a data card. Redundant routines, performing the same operations as the main routine can be added, with checking done to assure that the same routine is being run. The programs can also be provided with a parameter indicating the number of times the program has been run. This number should match with the corresponding log book entry.

5. Physical Control of Discs, Tapes, and System Control Cards

The physical control of computer system operational control media is fundamental to processing integrity. These media are vulnerable to theft, destruction, or unauthorized modification. They should have both machine-readable and human-readable labels.

Human-readable labels for tapes and discs can consist of color-coded and alphanumerically identified adhesive strips. These should be placed on the discs and tapes themselves as well as their containers. Machine-readable labels for tapes and discs should include a serial number, a code for the contents of the item, a version number, a date, and a protection code. This information should be read by the operating system before use, and as the reading by the system is done, a message should be printed on the system printer requesting the operator to insert into the input console the human-readable label. The result of the computer comparison of the machine-readable and human readable labels should then be reported on the system printer.

The punch-cards referred to in this section are system control cards in contrast to the application-dependent header cards and partial-election-result cards whose control was discussed in section V.E. Effective Control of Ballots and Computer-Based Election Records. However, the basic concepts are the same. These system control cards should have a use code and version number punched in identification fields (historically columns 73-80). Each card should be checked for proper use and version when read by the operating system and the effect of the card on system operation reported on the system output printer.

6. Logging of Operations

An important operations control tool is a log of all significant occurrences. In the computer room, two logs must be maintained. The operating system of the computer must be programmed to automatically report on the system printer all actions and their times of occurrence that have been taken by operators to change computer operating conditions. The operators themselves must, in addition, report in a log book all significant actions that they have taken and their

times of occurrence with respect to altering computer operation in any way, including the mounting and dismounting of discs and tapes, connection and removal of peripherals, insertion of data from the console or on punched cards, and the change of control switch settings.

These records, when vote-tallying is being done, should be included in the official records of the election.

7. Aspects of Internal Control

The general problem of security of computer programs, systems, and installations from natural and human hazards are well covered in two recently issued manuals, Federal Information Processing Standard 31 (FIPS 31), Guidelines for Automatic Data Processing Physical Security and Risk Management,[97] issued by the National Bureau of Standards, and the AFIPS Systems Review Manual on Security. The latter has been previously referenced.[96] Implementation of their recommendations should be given the most serious consideration when they are pertinent to vote-tallying. Some concerns worthy of specific mention here are division of personnel responsibility, and procedures for change controls on computer programs.

To quote from FIPS PUB 31 on division of responsibility: "One of the basic principles of internal control is to divide the execution of critical functions between two or more persons, a technique often referred to as separation of duties. The theory is that errors are less likely to go undetected when several people review the same transaction and fraud is deterred if there is a need for collusion. One individual should never be totally responsible for a given activity especially if it relates to the processing or development of sensitive applications."[98]

One application of this principle in the processing of election returns is the control of computer operation. More than one person should be used for this sensitive function. A second application is in the separation of duties between system operation and program design and modification. Separate individuals should be used for these tasks.

On the subject of control of program changes, FIPS PUB 31 states that "the process of getting a program from test to production status exposes the system to compromise from unauthorized changes and to loss of data integrity caused by too hurried development or inadequate testing. The ideal approach to installing a change in a production program is a formalized system in which several different organizational functions are involved."[99]

The inclusion of audit trails in the programming process, is recommended by FIPS PUB 31. "Every change [to a program], even those involving only one statement, should be authorized, approved, and documented with no exceptions. Otherwise, control is lost and the programming process becomes anarchistic,"[100] the manual states.

G. The Use of Teleprocessing

Teleprocessing has come into very widespread use during the past decade to provide access to or from computers at remote terminals. Timesharing computer service companies operate networks via ordinary telephone circuits that provide area-wide, nation-wide or world-wide computer and data base services to terminal users of many varieties. Specialized networks using teleprocessing include airline reservation systems, bank teller terminals and crime information networks.

The electrical transmission used in teleprocessing may be carried on wires, such as are commonly used for telephone or telegraph service; or it may be carried on radio, microwave, cable or wire high frequency carrier systems, or on narrow, directed beams or broadcast signals to and from earth satellites designed to relay or retransmit such messages.

The use of teleprocessing of ballot information to a remote computer site was noted in two counties visited by NBS representatives in the course of this investigation. These were Riverside, California, and Multnomah, Oregon. Other examples could be cited.

1. Advantages of Teleprocessing

Whether or not teleprocessing has an advantage over other methods of reporting depends on the specific situation. For precincts which are at long distances from a central counting site, there may be a payoff in speed of reporting of unofficial returns if sensors converting the ballots into electronic ballot images could be made available at those precincts. Whether to put the sensors at the central computer site or the precinct sites may depend in part, on the trade-offs between teleprocessing and physical transportation of the ballots to the central site, the controlling factors being speed, cost and management control.

If a ballot summarizer could be placed at each remote precinct, then a phone call reporting unofficial returns may be a viable alternative to teleprocessing of results from those precincts. The volume of information to be reported would be considerably less than if no summarizing capability existed.

For the reporting and certification of official returns, the justification of teleprocessing appears more difficult, since speed is not the controlling factor. Accuracy is the most important factor and the presence of official records from remote precincts, almost certainly requiring physical transportation from the remote precincts, is usually required in any event.

2. Accuracy and Security of Teleprocessing

Problems which must be considered when teleprocessing is used include those of accuracy and security. Accuracy means the ability to

receive exactly what was sent in the presence of natural noise phenomena. Security means the prevention of disclosure of the contents of the transmission to intercepters as well as the prevention of both deletion of the true contents and insertion of false data by persons intent on disrupting the system.

The efforts that should be expended to insure the security of the teleprocessing of election returns depend on the presence or absence of certain factors.

One of these factors is whether or not personal identification is being sent with the election data. Although no such system appears to be in actual use, an election system can be conceptualized in which a voter at a remote on-line terminal or telephone sends his or her choices to a central computer over telephone lines. In this situation, the voter might have to provide personal identification for authentication of registration along with the selections, thereby revealing his or her identity with the selections to an electronic intercepter. In fact, an experimental vote-by-phone system is being constructed in San Jose, California, under a grant from the National Science Foundation, but the purpose of the system is to be straw-vote issue referenda, not official voting.[101]

A second factor to be considered is whether the data are being sent before the polls are closed or afterwards. In some jurisdictions, early ballot collection is permitted, and in Multnomah County, Oregon, one of those jurisdictions, teleprocessing of ballots collected before the polls are closed occurs. Disclosure of ballot information before the polls are closed is illegal and electronic interception must be considered a security threat. Disclosure before the polls are closed may be used in attempts to affect the remainder of the voting.

A third factor to be considered, and this applies only to the situation in which the polls are still open, is whether the data transmitted are summarized or are in individual ballot format. If the data are summarized, an electronic intercepter knows immediately exactly what he wants to know, i.e., the status of the voting as of that time on election day. If the data transmitted are individual ballot information, the intercepter must sum up the data as well as capture it.

3. Technical Responses to Security Threats

Consideration should be given to several techniques including use of synchronous transmission and use of encryption.

Transmission of data is generally accomplished in one of two different methods:

(a) Asynchronous transmission. Each character contains the same number of information bits and each character representation is preceded by a "start" bit and followed by one or two "stop" bits. During

idle intervals the line remains in the "stop" condition. This form of transmission is typically used where the characters are generated by keyboards, since it accommodates an irregular occurrence of characters.

(b) Synchronous transmission. Each character contains the same number of bits (one or more), and "start" and "stop" bits are not used. There is no idle time between characters. The last bit of any character is followed immediately by the first bit of the next character. This form of transmission is used for fully automatic equipment. It gains speed by requiring fewer total number of bits transmitted per character. Because successive characters have their bit patterns immediately contiguous, synchronous transmission generally employs a block structure, where a block comprises either a fixed number or a variable number of characters per block. Some technique must be employed to indicate the beginning and end of each block. Usually certain bit patterns are reserved and used as "flags" to denote the end of the blocks.

A greater degree of knowledge would be required to intercept and alter a synchronous transmission than to intercept and alter an asynchronous transmission.

Encryption is the process of encoding the data being sent by replacing each symbol being sent by another symbol in a manner known only to the sender and receiver. Typically, an encryption device is inserted in the stream of data being sent over the transmission system immediately before the data reaches that system. A decryption device, which decodes the information and returns it to its "clear" form is inserted in the stream of data immediately after the data stream exits from the transmission system. Techniques and equipment for encryption and decryption have been used for many years, and with recent advances in miniaturization of logic elements, this equipment is now more cost-effective in providing data security.

Whether or not encryption and decryption is warranted depends on the situation. If transmission of summarized precinct voting results are to be sent over telephone lines before the polls are closed, then encryption should be seriously considered. Similarly, if personal identification is associated with individual votes sent over telephone lines, encryption should be strongly considered also.

If individual ballot data, not personally identified, is sent over telephone lines before the polls are closed, as is done in Multnomah County, the need for encryption must be weighed against the severity of the perceived threat. The psychological effect on the unsophisticated voter must be considered also. That voter who fails to understand computers and consequently fears their use in elections will likely understand encryption less and may be even more fearful. It is important, therefore, if encryption is employed, that information be disseminated to the public showing that the function of encryption is to protect the sanctity of the ballot and vote-tallying system security during teleprocessing.

An encryption algorithm, suitable for protecting transmitted data for any application and for any data format is now being considered by the National Bureau of Standards for adoption as a Federal standard.

For transmission after the polls are closed, the need for encryption due to the possibility of premature disclosure is eliminated. A remaining problem, which may affect transmission at any time, is that a sophisticated disrupter might be able to replace the correct information with false information on the transmission line, thereby causing the computer to receive and report erroneous results. The reporting of erroneous results, even if later corrected, may embarrass the election administration and reduce public confidence.

There are methods of encryption that can be employed to guard against insertion of false data into the transmission line. For example, an error detection code may be encrypted with each block of data, and the decryption error detector must match this code exactly, or else the system is aware that the data being sent is erroneous. This encryption application will detect either accidental or intentional errors in the data transmission.

To insure that correct results reach the computer for the certification of official returns, it is strongly recommended that a machine-readable record (e.g., magnetic tape) of what was sent be retained at the sending end of the transmission line. This record eventually can be carried to the computer location and run directly on the computer to verify what was received.

4. Accuracy of Teleprocessing

The assurance of the accuracy of transmission of data has been considered in detail over many years by communications engineers. Many varieties of error detecting and error correcting techniques have been devised. All of them employ "redundancy bits" added in some methodical manner to the message bits. The obvious goal is to discover a technique that will detect all errors with very few redundancy bits. This is not achievable, and a totally perfect error detector is not feasible. However, a detector having arbitrarily high detection capability is practical, provided there is sufficient detection time available; but a trade-off must be made considering block size, bit rate, channel noise characteristics, number of redundancy (check) bits, and the block transmission time.

Many data links are already in operation that employ a "check sequence" of redundancy bits appended at the end of each block of transmitted bits. These check sequences are generally in the range of 16 to 24 bits. They are referred to, besides check sequences, as "cyclic codes" or "polynomial checks" as well as by names of many inventors. The technique and its implementation using ordinary digital hardware was described in a 1961 article on "Cyclic Codes for Error Detection" by Peterson and Brown.[102]

It is recommended that in the teleprocessing of vote data, a cyclic redundancy checksum polynomial be appended to each block of data transmitted. Acceptable polynomial configurations include those known by the names CCITT (for Consultative Committee on International Telegraph and Telephone) and CRC-16. It has been reported that the CRC-16 polynomial currently is used in commercially-available communications adapters.[103] These polynomials are easily implemented in hardware and have been designed into programs. The CCITT polynomial has the status of an international standard and a study has demonstrated its superiority over CRC-16 for some error detection conditions and transmission configurations.[104] The CCITT polynomial also has been made available very recently for synchronous data link control.[147]

VI. MANAGEMENT OF THE ELECTION PREPARATION PROCESS

The difficulties in elections that have been reported make it clear that significant efforts must be expended to improve the management of the election preparation process. This is the process that results in the readiness of the vote-tallying system to perform as expected on election day. Some of the difficulties that can be classed as failures of election management, determined as a result of analysis of the descriptions reported in Chapter IV, are:

- failures to plan in advance for the timely completion of tasks;
- failures to issue effective operational instructions;
- failures to develop acceptance procedures for vendors' products and to insure that they are tested sufficiently before acceptance;
- failures to insure that subsystems are integrated into a complete working whole and that the entire system is tested sufficiently;
- failure to monitor and control vendors and to limit their activities to what is properly their sphere;
- failures to have contingency plans and back-up equipment;
- failures to recruit, train, and utilize adequate technical and administrative personnel; and
- failures to consider the motivational needs of employees.

Although the implementation of the instructions of management may require specific technical capability, it is election management's responsibility to insure that the technical competence exists, that it is organized, and that it is directed.

A. Election Preparation as a Developmental Activity

The kind of management direction that is needed in the process of preparing for an election may be better understood through consideration of the nature of the preparation process.

Although the voting and tallying activities on election day are operational, they are not operational in the same sense as other local government activities such as police patrolling, garbage collection, and voter registration. The latter activities are repetitious. They continue in relatively the same way every day, and may be considered as "production" activities. They can be quantified in outputs per unit time. A

characteristic of production activities is that they can be improved slowly over time in an incremental fashion because of their repetitious nature.

The vote-tallying system used on election day cannot be viewed as a production system. It is difficult to improve it incrementally over time because it is used infrequently during a short period of time. The preparations for an election have much more in common with a development project than they have with a continuing activity. The need for distinctions between management of developmental and repetitive activities is noted in the following quotation from the Journal of Systems Management. Here, manufacturing is used as the example of the repetitive activity:

"The manufacturing process is one of repetition, in which labor and other costs associated with each step can be measured over long experience and projected into the future with high confidence, subject primarily to changes in price levels.

"In recent years, there has been substantial movement in government, business, and industry toward the concept of projects. This does not suggest a change in the approach to manufacturing, but rather greater and more frequent cause of non-repetitive efforts. More prominent projects include the various NASA space programs, and development of new weapons systems. However, projects of more modest scale are being undertaken by numerous large and small organizations everywhere. Probably the most common smaller projects are related to automation, especially those involving the use of data processing equipment.

"These projects have in common the characteristic of being unique, one-time efforts. There is no exact precedent, and they will not be followed by a duplicate effort..."[105]

Although elections are duplicated, although following a definite hiatus, and the efforts in one election provide some learned experience useful in following elections, the viewpoint that management of the preparations for an individual election have more in common with NASA space programs than with manufacturing or police patrolling is a concept with considerable pragmatic value. An election is like the launch of a space rocket. It must be ready when needed at its deadline for completion, and it must work the first time. It is not surprising that several of the major difficulties reported in Chapter IV occurred the first time that a new kind of computing equipment was used in the jurisdiction.

The concepts that have been developed and utilized in the electronics and aerospace industries for the management of development projects with deadlines are applicable to the election preparation process.

In Figure 3 is an example of a network of sequence-related tasks adapted from one actually used in the aerospace industry in a

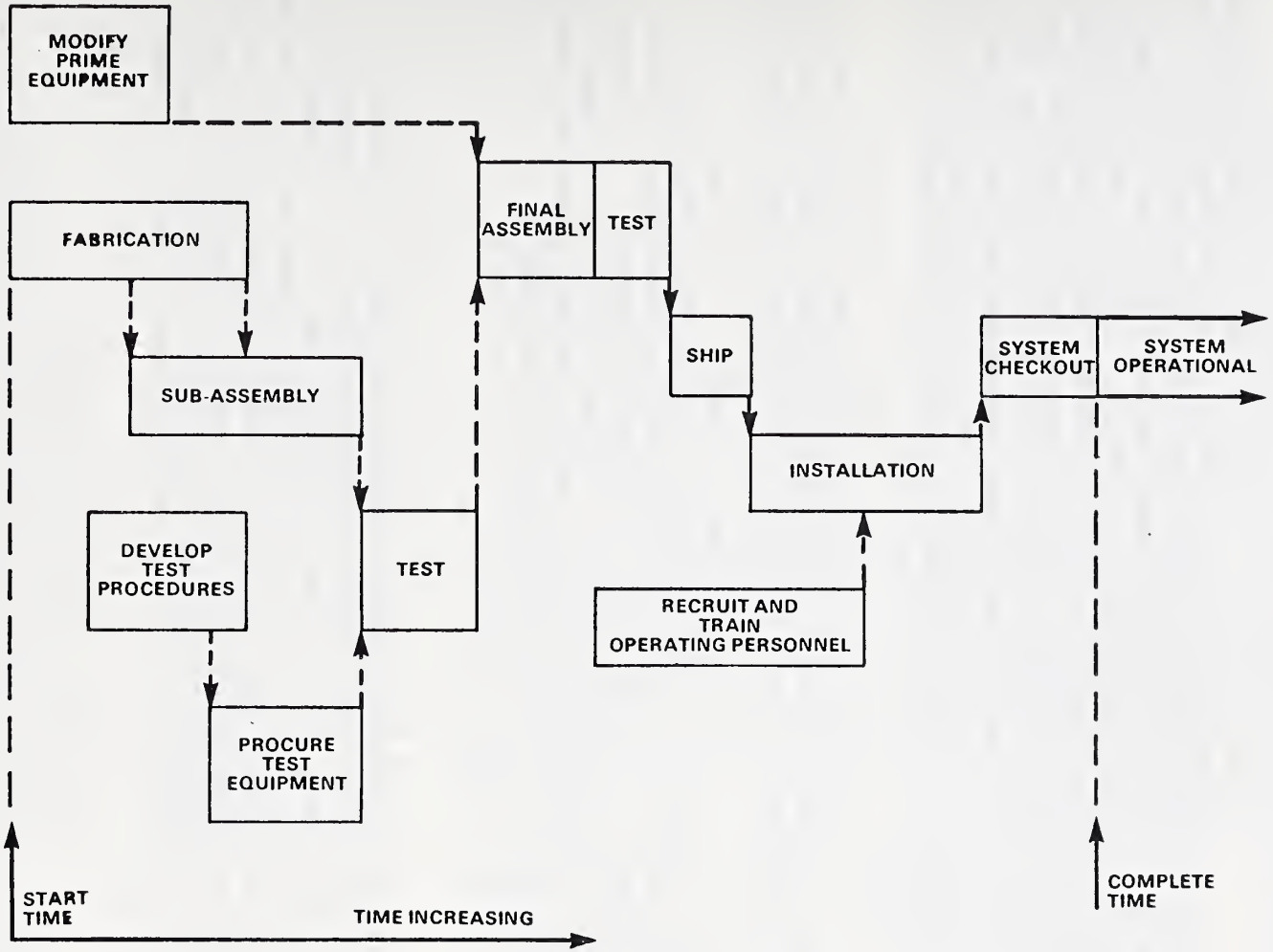


FIG. 3 A TIME-SEQUENCE NETWORK OF SYSTEM DEVELOPMENT TASKS

systems development project.[106] Of importance in this figure are the facts that a schedule of tasks is employed, that the system is seen to consist of components which are fabricated and assembled with what already exists, and that extensive testing and checkout are done.

The importance of a schedule encompassing the time sequencing of tasks in the preparations for an election was an important recommendation of the Economics Research Associates report produced for Los Angeles County in 1970,[89] and since that time Los Angeles has developed a very complete scheduling system. The State of Arizona, in its Instructions and Procedures Manual[107] also provides a complete schedule of tasks for the conduct of elections. The recommendations that a PERT-type elections planning and controlling procedure should be developed and that written procedures for every activity associated with the election process spelled out in step-by-step detail should be prepared were previously recommended by a report sponsored by the Office of Federal Elections of the General Accounting Office.[108]

There has been considerably less concern by election administrators on proper checkout of subsystems and on the integration of subsystems to form a working whole than on the development of schedules. Although a dry run of each activity associated with the conduct of an election has been recommended in the report just cited,[109] and in addition, a computer system test and review program was also recommended,[110] these proposals do not encompass the complete range of procedures envisioned here. Considerable emphasis is placed by this report on acceptance testing of computer programs and computers and other vote-tallying devices, as well as on the operational checkout of specific configurations of equipment to be used.

1. Three Step Process

In effect, a three step process for operation of vote-tallying systems is proposed. The first step is the acceptance of the hardware and software for future use, based on conformance with specifications. The second step is the operational checkout of the accepted components, including any modifications necessary to specialize them for a particular election in which they will be used, followed by a dry run of the integrated system. The third step is the actual operation of the system on election day and during the tallying process on election night. A thorough analysis, preceding these steps, is assumed.

B. The Computer Program as a Product

General purpose computers used for vote-tallying as well as ballot summarizers and electronic vote summarizers, have in common the fact that they are all programmable. It is the program, that is, the set of instructions and/or the settings of dials, switches, plugboards, and the like, that specializes the vote-tallying device to the particular election task that it must perform. Without the program, the device

would be inoperable, a useless conglomerate of expensive materials. As one well-known computer specialist has said about software, the collection of all programs used by a computer:

"Without its software, a computer is the electronic analog of a human vegetable."[111]

Of course, with the wrong program, a vote-tallying device is worse than useless. Its incorrect results cause confusion and delay, and the later the errors are discovered, the worse the situation. Clearly, the program with which a vote-tallying device operates, acts as an integral component of the device. When the program is changed, the logic of the device's operation is changed. In effect, the device, then, is logically a different device. The implication of this must be considered for the "approval" which programmable vote-tallying devices such as ballot summarizers and vote summarizers receive from the States.

If "approval" is a guarantor of accuracy, or a minimum is related to accuracy, the the program cannot be ignored. Since the program is changeable and is changed each election, there is a possibility that it may be incorrect. The approval process must consider the effect of the program in altering accuracy.

When punch-card ballots are used, the voting device which receives State approval, i.e., the ballot holder, is not programmable. The program is in the computer which processes the ballots; and although States require that logic and accuracy tests be done and that a copy of the completed program be sent to the State before the election, the computer and its program receive in most States no State approval or examination. The failure to consider the vote-tallying program for approval is a serious flaw, and may result from a misunderstanding of the nature of a program.

A vote-tallying program that is meant to run on a general-purpose computer is a fabricated product with certain characteristics and specifications. It is, in general, purchased or leased from a vendor with the understanding that it will accomplish a specified function. To the greatest extent possible, it must be subject to the same kind of acceptance checking which other complex products receive when they are purchased or otherwise obtained for government use. The certification by the "programmer" that no errors are contained within it, which is a requirement in one State, does not constitute a complete acceptance test.

It is true, of course, that a computer program is somewhat different from products that are normally found in "hard" form. The program may exist in a form invisible to the naked eye, e.g., on a magnetic medium, and in that form, it may be duplicated or altered outside its original place of manufacture for an extremely low cost. In addition, a program is convertible from its source code to a machine code. The latter appears completely different from the source code, but should be logically identical from the user's viewpoint.

These differences with "hard" products make a computer program more difficult to specify, test, and control, but do not obviate the necessity for doing so.

C. Design Specifications for Vote-Tallying Programs

The most important quality that a vote-tallying applications program must possess is that it must operate correctly. At first glance, this may appear to be simply stating the obvious, but upon further reflection, it should be understood that it is not exactly a simple matter to state what is meant by correct, and it is extremely difficult to prove that a program does indeed possess this quality. (See example of Redford Township, Chapter IV.) Correctness implies, of course, that correctly marked ballots, in which only valid locations are marked and in which no overvotes are marked, are summed correctly; but it also implies that the program does exactly what the election administration intends it to do with ballots that are not so "well-behaved." The program must ignore marks or holes on ballots in locations which have not been assigned to any offices or issues without affecting marks or holes in assigned locations (if that is what the administration intends) and it must throw out overvotes for offices or issues in which they occur without affecting the program's performance on correctly-voted offices or issues of the same ballot.

1. Use of High Level Language

To assure correctness, it is important that a vote-tallying program be designed to maximize its clarity or intelligibility and to maximize the ease with which it can be tested for correctness. It is generally agreed by most authorities that programs meant for a general-purpose computer written in a high-level language, for example COBOL, FORTRAN, or PL/I are considerably easier to understand than those written in an assembly language or directly in machine code. It should be noted that there are existing national standards for the COBOL,[112] FORTRAN,[113] and Basic FORTRAN[114] languages available from the American National Standards Institute and that the COBOL standard has been adopted by the Federal government.[115] In addition, programs written in a high-level language are more likely to be transferable among different manufacturers' machines, thereby reducing governmental efforts needed for acceptance testing.

2. Documentation

Documentation, including listings, flow charts and interspersed comments among the statements of the program, provides further clarity and is needed to assure effective examination of the program during acceptance testing.

The use of a high-level language and clear documentation is particularly important if there is a requirement that candidates or their representatives be given the opportunity to review computer programs.

Candidate representatives can, in a considerably shorter time, understand a program meant to run on a general-purpose computer that is written in a high-level language for which extensive flow charts and comments have been provided than is likely with any other program configuration. Confidence in the election process will thereby be improved.

3. Use of Table-Driven Programs

The concept of an acceptance test for a program implies that once accepted, the program may be used in all succeeding elections provided no change in the basic logic structure occurs. It is important therefore, in order to minimize the need for repetitive acceptance tests, that the basic logic structure of a program remain fixed. This is possible if the concept of a table-driven program is adopted. With this type of program, the parameters which define the correct analysis of any ballot are put in a set of tables. Some of the data which might be put in tabular form include: the set of offices and issues for which each precinct votes, the set of ballot locations corresponding to each office and issue, the candidate rotation for each office voted in each precinct, the maximum allowable number of votes for each office, and the names of the candidates or responses for each office and issue. The program logic could be such that as soon as it receives the precinct identification of any ballot, the contents of the tables to which it is directed determine how the program logic is to analyze the contents of the ballot and add its votes to summary tables of results.

The advantage of a table-driven program is that once its logic is checked out, it is less likely to retain undiscovered residual errors than a program whose logic must be altered each election. At the present state-of-the-art, a major method of assuring correctness of programs is to run them over and over again with different inputs. A program whose basic logic must be altered each election does not allow for repetitive operational checkout. In addition, a program whose logic must be changed for each election requires more programming labor over the life of the program; and typically for each election, more time must be allowed for its modification.

4. Inclusion of Audit Trails

In Chapter V, methods of providing documentation of ballot and vote allocation were described. In addition, certain protection procedures for controlling election records either used as computer input or resulting as computer output were proposed. These proposals impact the design of a vote-tallying program.

Specifically, the following capabilities would need to be possessed by the program in order to implement the proposals of Chapter V:

- capability to provide the number of ballots machine-counted for each precinct,

- capability to provide the number of overvotes and undervotes for each office, in each precinct,

- capability to provide the partial sum of district wide-totals following the addition of each individual precinct into those totals,

- capability to read the precinct number from each ballot and check the validity of the number read,

- capability to copy out on the output printer the exact contents of each header and other control card read at the input, and

- the capability to read out the list of candidates for each office in each precinct in the same rotational sequence as they were listed in the instructional materials for that precinct.

5. Use of Modularity

The use of modular design of computer programs is one aspect of good software engineering. Modular design implies that a program is built as several self-contained elements. The functions of input and output are well-defined for each module, and each module has a single entry point and single exit point.[116]

The basic reason for the use of modularity is to subdivide a complex problem into separate, smaller, more simple problems. Modularity makes a computer program more easily subject to analysis. Furthermore, with true modularity, it should be possible to modify any module without affecting any other module, as long as there is no major redefinition of functions that affects the relative contents of two or more modules.

The use of modularity might help allay certain suspicions that have been raised about errors that could exist in vote-tallying programs. It has been suggested that the use of a small-size logic and accuracy test opens the possibility that a vote manipulation could begin to occur in a vote-tallying program after the number of ballots used in the logic and accuracy test has been counted. Thus, the vote manipulation program segment would not be found by the logic and accuracy test, it is claimed.

Guarding against this kind of program falsification is aided if the vote summarization activity is separate and distinct from other parts of the vote-tallying program. One might envision, as an example, three basic program modules: a ballot analysis module, a precinct summary module, and a district-wide summary module. The function of the ballot analysis module would be to determine the content of an individual ballot and to prepare its allowable votes for summation

to the correct storage locations of the precinct summary module. The precinct summary module would contain, in separate tables, the current summed votes for each precinct. The program logic of this module would prepare the precinct totals for correct summation to the district-wide office totals and would provide print-out capability for each precinct's totals individually. The district-wide summary module would contain, in separate tables, the current summaries for each office and issue, district wide. The logic of this module would provide print-out capability for district-wide vote totals by each office and issue.

The philosophy of design just enunciated allows for audit capability by individual precinct, and any successful vote manipulation scheme attempted on a program with these audit trails implemented would have to involve manipulation of individual precinct totals and/or individual ballots contents, not just a single wholesale vote switch. The modularization makes clearer the type of testing which must be done to assure correct logical operation of each program path. It implies that each precinct's ballot arrangement and summarization steps must be checked out. The modularization also permits a method of program testing in which the inputs and outputs of each module can be separately subjected to logical analysis. Outputs of each major module should be capable of being printed out.

6. Provisions for Testing

A useful design specification to impose is for the program to be able to receive inputs of ballot images on magnetic tape or disc, as well as standard machine-readable ballots. This requirement insures that the program can be quickly tested with a full simulation of the largest number of ballots which any jurisdiction using the system expects to receive.

7. Programs for Special-Purpose Devices

The previous discussion has assumed that the vote-tallying program is intended for operation on a general-purpose, stored program computer. This type of computer has a main memory allowing both reading and writing, a repetoire of elementary machine instructions which causes data to be moved among registers and/or storage locations and can cause logical and arithmetic operations on the data, and typically executes programs by taking instructions in numerical sequence except when caused to "jump" or "branch" to the start of a new sequence. Almost all commercially available digital computers found in general government and business installations are of this type, even if the computer is called a "minicomputer." This type of computer is generally provided with a supervisory program or operating system by its manufacturer and the support software almost always includes a compiler. The compiler converts the applications program written in a high-level language (e.g., COBOL or FORTRAN) into a sequence of elementary machine instructions and storage locations useful for the particular machine on which the applications program is to run.

The ballot summarizers and electronic vote summarizers discovered in use during this investigation (see Chapter III) are not general-purpose stored-program computers, although they all require some form of programming to specialize them for a particular election and ballot configuration. Their programs cannot be required to be written in a high-level language. The concept of modularity does not apply, and the items listed under VI.C.4. Inclusion of Audit Trails require further interpretation in connection with these devices. Discussion of these programs and audit controls that are reasonable to apply are covered in section E.4. of this chapter.

D. Acceptance Testing of Vote-Tallying Programs

The test used to accept a vote-tallying program should involve a simulation of realistic conditions as much as possible, coupled with a checkoff of the design specifications which were imposed.

The vendor of the program should be requested to identify all the hardware configurations with which the program is intended to operate, and also identify the maximum values of election parameters which the program can support. These parameters may include the maximum numbers of precincts, offices and issues, candidates per office, etc.

The simulation of vote-counting for the purpose of acceptance testing should involve a configuration of numbers of voters, precincts, offices and candidates which tests the maximum capabilities of the program. Simulated ballots (through the use of ballot images on tape) should be used to more quickly evaluate the logic of the program. (Actual ballots should also be used but the use of a full complement is time-consuming and expensive.) The simulated ballots should include those that are "well-behaved" involving no overvotes or marks in unassigned locations as well as some that are not so well-behaved. It should be assumed that voters will configure their ballots in every conceivable way and some ways which are highly improbably but possible, nevertheless.

If the acceptance test is intended to approve the program for use with several different hardware configurations, then a test of the program with each configuration is called for. Various election arrangements of different numbers of voters, precincts, offices and numbers of candidates should also be tried.

1. Use of a Ballot-Generating Program

For the purpose of developing a tape of randomly-configured ballot images, a computer program is a valuable tool. This latter program is effectively the inverse of the vote-tallying program under test. The tape-generating program starts with a set of results for every precinct and every office and issue and decomposes the results into a set of

ballots, including some which involve overvotes, undervotes, and invalid votes in as many different combinations that are humanly possible to program into it. Hopefully the results with which it starts will be matched by the results obtained by the vote-tallying program under test. Barring defects on the tape of ballot images, the results should match identically, since the accuracy of the actual ballot sensor is not a factor in the test.

The ballot-generating program may also be used to generate actual ballots as well as a tape of ballot images. With actual ballots, the accuracy of the sensor is involved, and some small number of errors is determined by the design specifications imposed on the sensor. This subject is covered in the next section.

The ballot-generating program is one that is needed, but does not appear to be generally available. If produced in one jurisdiction, preferably in a high-level language, its transfer to many other jurisdictions would be a valuable undertaking.

2. Acceptance Test Contrasted With Pre-Election Checkout

It should be understood that the acceptance test is not intended to be the same as the pre-election checkout. The acceptance test is for the purpose of certifying the program for use, and therefore should involve tests under varying conditions, not necessarily those specifically found in any particular election. As a result of the acceptance test, some of the general capabilities of the program should be identified and communicated to its future users. These capabilities will include its storage requirements, its speed of operation with different equipments, and any special parameter alterations that can be programmed into it or modifications that can be inserted.

The program should be able to have its print-out capability altered to provide speed for unofficial results and full audit capability for official results to be certified.

The acceptance test approval should be granted not less than several months (three or more) prior to the program's first use in an election. The purpose of this waiting time is to insure that a jurisdiction is not committed to a program that cannot pass its acceptance test and so that the jurisdiction has sufficient time to select an alternative voting procedure.

E. Design Specifications for Equipment and Supplies

Equipment and supplies used in computer-based elections are of a varied nature, but they can be put in a set of specific categories. The following list of categories may not be exhaustive but it includes most of the important items that are special to the election process:

- ballots,
- ballot encoding equipment, including ballot holders, ballot punches or styli, pencils, ink stampers, stamp pads, etc.,
- instructional supplies, including ballot holder inserts, sample ballots, procedural instructions issued to precinct officials and voters, etc.,
- election audit forms and records, including those that account for delivery and receipt of ballots, registration verification, ballot duplication and spoilage records, computer output results, etc.,
- ballot transportation equipment, including metal transport cases, and plastic bags to prevent precipitation damage,
- sensor equipment, including punch-card readers and mark-sense readers, either separate or integrated into computing equipment,
- data processing devices, including general-purpose computers and summarizers, computer peripheral equipment such as mass storage units and printers, and teleprocessing equipment, and
- data processing supplies, including tapes, discs, cards, and printer paper.

1. The Need for Specifications

The varied list presented above is indicative of the complexity of election administration. Some of the design specifications that need to be imposed may be quite elementary (e.g., for pencils for marking ballots); but others need to be quite technical and may require some exploratory investigation to insure that the imposed requirements are both necessary and sufficient to insure an accurate and well-run election.

Many election difficulties that have been reported have been ascribed, in part, to failures to impose adequate design specifications or to verify that they have been met, if imposed. For example, as noted in Chapter IV, punch-card ballots that were of two different lengths caused difficulties in Washington Township, New Jersey in 1973 and ballots of an incorrect thickness caused problems in the District of Columbia in 1971. Failures to impose adequate design requirements on ballot holders were believed to have caused ballot mispunchings by voters in Detroi in 1970. Card reader jams believed to be caused by excessive quanti es of chad falling from punched card ballots were

reported in Detroit and Los Angeles in 1970. Vacuum-feed card readers, in general, handle pre-scored cards with fewer jams than mechanical-feed readers. Defective magnetic tapes, employed to record ballot images, were believed to have caused difficulties in the District of Columbia in September, 1974. Different sensitivities of mark-sense readers also caused difficulties in the same District of Columbia election in 1974.

The fact that a device is simple does not eliminate the necessity for imposing some design specifications. A pencil for marking ballots, if too light, may not provide enough discrimination for the sensor, and a pencil that is too dark or one that includes an eraser may produce smudges that cause the sensor to record incorrect results. Metal ballot transport cases with poor locking mechanisms may open, thereby spilling the ballots, or if not designed to close tightly may allow precipitation to enter, thereby damaging the ballots. Election administrators ought to employ the rule that if anything can go wrong it will, particularly if insufficient management attention has been paid to it. Imposition of design specification is an important management tool that ought to be employed to its fullest capability.

2. Specifications for Sensors

The sensor, the device which converts information on a ballot to electronic form for data processing is one of the key elements of a computer-based vote-tallying system. Its accuracy and reliability must be unquestioned. Furthermore, the accuracy of a sensor cannot be considered by itself. The detectability of the data supplied must be included in the accuracy determination. In effect, the ballot, the vote-encoding equipment, the voter, and the sensor form a sub-system causing the voter's choices to enter the data processing part of vote-tallying. Coordination of design specifications among the ballot, the vote-encoding equipment and the sensor is of paramount importance to overall vote-tallying system accuracy.

Design specifications for a sensor may be put in statistical terms. These terms concern the probability of error, and there are two kinds of errors. There is the error of reporting no mark or no punch when one is present, and there is the error of reporting a mark of punch when actually none is present. Values for these probabilities of error should be established. Determination of whether or not a sensor meets these specifications in coordination with expected data input quality is discussed in the section on acceptance testing.

An important specification for a sensor concerns its effect on ballots that it reads. This effect must be minimal in case the ballots must be re-read. Specifications also should include concern over the sensor's stability over time in its working environment.

3. Specifications for Electronic Equipment

Electronic components such as sensors and computers may be subject to changes in parameters over a period of time. These changes may be due to aging of components, changes in power supply value or quality, especially high or low values of humidity or temperature, dust in the air, or electrostatic charges on rugs.

The kind of specifications that should be imposed depends in part on the environment in which the equipment is to be located. Precinct-located devices which may be placed in non-air-conditioned spaces may require different specifications than other equipment placed in controlled environments. The environment of the warehouse, where the equipment may be stored for a long time must be considered.

Reliability and availability are parameters with which jurisdictions need to be concerned. Mean times to failure and mean times to repair, the availability of spare parts, (both short term and long term) and the availability of maintenance assistance during the critical vote counting hours, the effect on equipment as a result of shock e.g., due to being dropped while in transport, are some of the parameters which ought to be considered in establishing design and procurement specifications. At present, California may be the only State in which some design specifications, not determined by the vendors themselves, are imposed on electronic equipment. For example, that State has issued a Reliability Demonstration and Test Specification for Electronic and Mechanical Vote Recording and Tabulating Equipment.[117]

Security considerations are another aspect of design specifications which ought to be considered. Aspects of this question have been covered in Chapter V, but new systems are being proposed in which different questions of security may need to be reviewed.

For example, with precinct-located voting devices, there must be a concern that the voter cannot, in any way, be identified with the specific votes he casts. It has been noted that it is important to insure that the voted punch-card ballot is covered while its stub is being removed. In addition, there should be a consideration of whether sounds or electromagnetic radiation emanating from the voting device are of sufficiently high magnitude to permit a person or an external detector coupled with some data processing facility to relate the emanating signals to a specific vote pattern. If the voting device employs only transistorized electronics and low-level signals, this is not a problem. It may be a problem with mechanical or electromechanical devices.

Similarly, a magnetic tape, if not employed in a secure environment, ought to be enclosed within a case to insure a physical separation from a source of a magnetic field that could affect it. A data tape surface is relatively secure from arbitrary erasure by a hand-carried permanent magnet if it is located no closer than about 76 millimetres (about 3 inches) to any point at which such a magnet could be placed. NBS has issued a report on this subject.[4]

4. Design Specifications for Summarizers

An important aspect of ballot and vote summarizers is that they are altered to specialize them for each election. Specifications should include the methods that are used to document these changes so that the documentation can become part of the election records.

Audit trails are needed in these devices, just as they are in computer programs meant for stored-program computers. If summarizers are precinct-located, the capability to provide partial summations of district-wide totals following the addition of each precinct is not a pertinent requirement. Nevertheless, the other capabilities listed under VI.C.4 Inclusion of Audit Trails are still pertinent. However, the provisions for some of these capabilities, for example for undervote storage and the computation of undervotes for offices in which more than one vote is allowed, would probably need to be implemented in hardware in these devices. The extra cost of this implementation must be weighed against the need for complete confidence in the results.

F. Acceptance Testing of Vote-Tallying Equipment

The concept of acceptance testing implies that there exists a group of identical devices, and some subset of these are to undergo a specific test determining whether design specifications are met. If those undergoing the test pass, then it is assumed that the remainder, designed identically will also pass the same test and be allowed to be used. If the number of devices is small, say ten or less, then perhaps each one may be required to undergo specific acceptance tests against design specifications. If the number of identical devices is larger, then a small number may be required to undergo extensive tests and the remainder limited to tests on the most fundamental parameters. If the number of identical devices is very large, sampling techniques may be employed, in which some small group is arbitrarily selected for test at discrete time intervals and the vast majority of the identical devices undergo no test at all. There is clearly a trade-off between the complexity and importance of a device and the time spent in testing it. Fortunately, economics also dictates that the more complex a device, the fewer of them there are likely to be, so that more time can be afforded in testing it.

As has been pointed out, a key device in vote-tallying is the sensor, the device converting ballot information to electronic form. The sensor may be tested first against an "ideal" ballot, that is a ballot with the best data quality, possibly generated by machine. If the sensor cannot meet accuracy requirements in this situation, there is no point in proceeding further.

Even if the sensor meets specifications under ideal conditions, it will not be used under ideal conditions. In an election, the system is to be used by voters of varying abilities. The concept of the vote-tallying system must be that it is there to serve the voters, and the

system must be geared so that the overwhelming majority of voters, approaching 100%, can use it to record their votes as they intend.

Thus the ballot, vote encoding equipment, sensor combination should be given an acceptance test under simulated voting conditions, using a statistical sample of voters. It can be determined in this manner if sufficient overall system accuracy can be achieved. The accuracy specifications established for the sensor assuming perfect data input quality will need to be relaxed to establish overall system accuracy specifications, but clearly, if too many voters, told beforehand how to operate the system, cannot have their choices recorded correctly, the system must be rejected.

What is being proposed here is a controlled experiment involving the human element in the voting process. Such experiments, if they had been carried out when punch-card systems were first introduced, might have made clear the difficulties caused by hanging chad on ballots, loose design specifications for ballot holders, and card reader jams that plagued such systems initially.

1. Acceptance Test Input to Pre-Election Checkout

A major result of a successful acceptance test should be a document communicated to those people who will perform pre-election checkout. This document should describe how each approved device should be demonstrated to be working acceptably.

G. Pre-Election Checkout of Vote-Tallying Systems

The obvious purpose of a pre-election checkout is to insure that all components of the system, including equipment, supplies, and personnel, are in readiness for actual operations on election day and election night. A developed PERT diagram should be an aid in the checkout. There should be a certainty that all supplies have been delivered, that all needed personnel are assigned, know their duties, and that all equipment is in working order. Instructions on assuring correct operation of equipment, developed as a result of acceptance tests, will assist in this process.

1. Computing Equipment Checkout

Computing equipment, specifically, should be exercised, to determine that there are no undiscovered program bugs or other malfunctions. A full simulation of the total number of ballots to be expected (using a tape of ballot images) should be done, if at all feasible. If this had been done in Clackamas County, Oregon, in May 1974, the minor difficulty reported in section IV.B.7 concerning that County would have been discovered beforehand. Similarly, the error in the print program in Riverside County, California, in their 1974 spring primary which caused some digits of certain results to be initially omitted, would not have

had to be reported.[118] A more complete pre-election checkout might have prevented the computing difficulties in Travis County, Texas in November 1972, reported in section IV.B.4.

A minor difficulty that occurred in the District of Columbia general election of November 1974, was that some of the power outlets in the school buildings in which ballot summarizers were located were old and worn. This problem, causing interrupted power supply, would have been discovered by a pre-election site check with the equipment to be used there.

Sensors are among the equipment types that should be given specific and intense attention.

2. Ballot Rotation Checkout

An important aspect of computer program checkout, and also for checks on the instructional supplies sent to voters and precincts, is correct ballot rotation. There should be a certainty that the sample ballot delivered or handed to a voter matches the ballot arrangement that the voter will find in the polling station. Similarly, there should be a certainty that the ballot rotation the computer system is expecting is exactly that which is on the ballot instructions in the polling station.

3. Personnel Activities Checkout

A pre-election checkout will help operational personnel to be more certain of their duties. The minor difficulty that occurred in King County, Washington, in 1973 (see section IV.B.6) in which certain program control cards were not inserted correctly in the computer might have been prevented by more attention to personnel duties. The failure of one computer operator to follow instructions in the District of Columbia primary in September 1974, as reported in section IV.A.7, was a major cause of difficulty in that election. "Educating the people who must work with the system becomes the single most important factor in computerizing the vote count," is a comment attributed by Computerworld to the registrar-at-large for Hamilton County, Tennessee.[119]

4. Contingency Plans and Back-Up Equipment

Pre-election plans must consider situations which will not go as initially expected. Spare personnel must be held in readiness to man uncovered stations, wherever they might be. Spare parts and supplies must be available. Officials in remote locations having difficulties must know how to get help.

Failure of centralized computing equipment must be considered a possibility, and alternate sites held in readiness. In Chapter V, machine recounting was proposed, and the readiness of a back-up site may provide the independent recounting site that was recommended. Interjurisdictional agreements, each providing back-up capability and recounting capability for the other should be given serious consideration. However.

a problem of security of the ballots may exist if they are removed from the County in which they are being voted. This question is further discussed in Chapter VII.

H. Assurance of Management Control

An important aspect of preparations for an election is the assurance that the chief local elections administrator will have full management control over all the resources which he or she will need to utilize. These resources include the personnel, the equipment, the supplies, and the sites involved.

In Detroit, in 1970 (see section IV.A.4) a difficulty with serious consequences was that there was not full management control over sites and computer equipment at those sites. According to reports, the computer sites, which were borrowed on election night from private companies, had to be returned to those companies the next morning, before election processing was complete. Furthermore, because of the security controls imposed by some of the private companies whose computers were being used, candidates' observers were not permitted to view the proceedings. This was reported to be in violation of Michigan election regulations.[31]

In other cases, vote-tallying programs have been run on computers on which other programs were being run concurrently, with multiprogramming. The computer equipment, the support software and the operational personnel were not under the control of the elections administration. Typically, the computer is under the control of another general government department, and emergency police services and hospital services may be permitted from remote terminals using multiprogramming during the testing and running of the vote-tallying program. Entry into the computer room and operation of the equipment are under the control of the computer center manager who may not be responsible to the elections administrator. The center manager may control entry according to his instructions from his superior and he may operate the computer according to his own superior's priorities.

When vendor's representatives take an active role in election night processing, conflicts of interest may arise if activities do not go according to plan. In one situation, local election officials charged that the vendor of the computer program and equipment, who was also operating the equipment on election night, refused to give to the election officials certain computer print-outs, which were clearly election records.

The proper procedures, which protect both vendor and election officials and which make clear the responsibilities each has, must be worked out in advance. The vendor should have his own checkout procedures which he should document. These procedures might be the subject of a prior agreement between the vendor and the elections administration. When these checkout procedures are completed, the equipment and the

responsibility for operating personnel supervision should be turned over to the elections administration, even if the operating personnel are normally employed by the vendor. If the equipment malfunctions during vote-tallying, (or appears to be malfunctioning) transfer of control back to the vendor according to pre-arranged agreement is a reasonable procedure. This concept of supervisory control is important to properly divide responsibility for vote-tallying and equipment supply between the elections administration and the vendor. The elections administration must assume responsibility for all vote-tallying activities. If it does not, or it cannot because it does not have the expertise to do so, it is not fully carrying out its assigned governmental duties.

The vendor, on the other hand, ought not to assume any responsibility for vote-tallying. To do so would be to assume a governmental function which the vendor is not entitled to assume. Prudence should dictate that the vendor should limit his involvement to the supply of fully operational equipment. If the vendor supplies personnel, then the specific training which these personnel receive prior to the start of vote-tallying should be the subject of prior agreement, and during vote-tallying these personnel ought to be under the supervision of the elections administration.

VII. INSTITUTIONAL FACTORS AFFECTING ACCURACY AND SECURITY

A. The Need for Statewide Specifications

In previous chapters, recommendations have been made for improving the accuracy and security of the vote-tallying process and for improving the management of election preparations. Actual implementation of those recommendations concerning the vote-tallying system operation and pre-operational checkout are the responsibility of local election administrators. Other recommendations have concerned design and documentation controls and acceptance testing of elections hardware and software.

The feasibility of implementation of the latter recommendations on the local level is questionable. As the Council of State Governments concluded in its report Power to the States - Mobilizing Public Technology:

"There are striking examples of a ready response by industry... to share know-how in tackling complex problems of government. But industry hesitates to risk capital in developing targeted products and services for a market that is fragmented and disaggregated and which is not organized to structure and maintain effective demand."[120]

The problem of market fragmentation and its effect on the imposition of locally-imposed design controls must be considered. A single local jurisdiction, desiring to implement design controls over the products it purchases or leases has little chance of obtaining its desires in a cost-effective manner due to its lack of market leverage. A single jurisdiction typically must choose among those products already in the market place, selecting the most appropriate mix of cost, performance, and other valuable characteristics that are presently available. Economic factors often prevent special procurements.

It must be concluded, therefore, that only at a higher level of government than local, i.e., at the State level or higher, is there significant aggregation of demand to obtain the cooperation of industry to make available products with the desired characteristics. The referenced Council of State Governments' report suggests that multi-state arrangements would be even more effective. "To the degree that state governments are willing to agree on product standards and performance criteria and to combine their purchasing leverage on industry through new arrangements of a multi-state or regional character, industry's readiness to respond with technological innovation will be decidedly better,"[121] the report concludes.

At minimum, then, some State actions in assuring desired product design and documentation characteristics are a necessity. This does not necessarily imply actual State purchase of all systems, simply State-imposed design and documentation features. Thus, the following recommendations of Chapter VI will have considerably more chance of adoption if implementation is imposed at the State level:

- design and documentation requirements for all computer programs that are to be used in any stored-program computer employed in an election system;

- documentation requirements for all changes in the logic of computing devices used in a vote-tallying system, particularly when those changes are performed in the process of specializing the devices for a particular election; and

- acceptance specifications and testing of all software and hardware before they are permitted to be used anywhere in the State.

B. The Need for Local Technical Expertise

A second problem in successful implementation of the recommendations of the previous chapters is the availability of computer technology expertise to local election administrations, particularly those not well-funded or those distant from large metropolitan centers where such expertise is more likely to exist. One result of the lack of available expertise is that vendors of computer programs and hardware, in many cases, conduct a significant part of the election on the jurisdictions' behalf. As a result, jurisdictions may not be able to enforce the necessary guidelines to insure accuracy and security, and even may not be aware of these guidelines. Furthermore, when vendors assume more responsibility than they should, due to the jurisdictions' lack of in-house capability, situations may be created in which conflict of interest is a serious concern.

The recent report of the National Municipal League (NML) entitled A Model Election System comments that "State election officials agree generally on the need to upgrade election procedures by providing more technical guidance to local officials, particularly in such areas as the utilization of electronic data processing techniques."[122] The State of Oregon Elections Division provides a systems analyst to each of its local jurisdictions in the conduct of each Statewide election. It may be the only State to do so at this time.

Mrs. Marie Garber, Elections Administrator of Montgomery County, Maryland, in commenting on the NML report, notes "What strong state control can provide is direction to localities, many of which are neither funded nor staffed to make improvements on their own initiative."[123] It is concluded, therefore, that each State, by providing manpower and/or funding, should insure that each of its jurisdictions has sufficient managerial and technical expertise in its employ, augmented by independent consultants if necessary, to carry out its statutory responsibilities without primary reliance on representatives of vendors of election system components.

C. The Need for Uniformity

One result of differences in the availability of local technical expertise is a lack of uniformity in the imposition of accuracy and security guidelines. In earlier, less technologically complex times, regulations such as requirements for the secret ballot and voter registration were implemented. These regulations are recognized today as fundamental to the sanctity of the voting process, but they were the accuracy and security guidelines of their times. The guidelines concerning the use of computing technology that need to be imposed today must be recognized as the logical extension of the earlier, more fundamental guidelines, and the need for uniformity is no less important now.

The need for uniformity and State leadership were two of the factors that caused the League of Women Voters Education Fund as well as the NML to conclude that State responsibility for elections should be centralized in a single State office or official. The League of Women Voters report Administrative Obstacles to Voting recommends "that the state election official establish and issue to every local election official minimum standards and performance guidelines; that the state official also establish a supervisory structure within which he or she can evaluate the performance of local officials under the guidelines and take corrective action where the standards are not being met." [124] The same report also recommends "that the state authority conduct mandatory training sessions which cover ... the technical aspects of efficiently managing an election system..."[125] The NML report A Model Election System similarly recommends that "The Chief [State] Electoral Officer should provide written standards and directions to county administrators for carrying out local responsibilities for registration and voting"[126] and "the state should develop training programs for precinct personnel and other election employees."[127]

However, uniformity is not seen as a universal good if it prevents advanced jurisdictions from providing more than the minimum requirements or it stifles innovations. Note that the quotation above from Administrative Obstacles to Voting asks for "minimum standards and performance guidelines." Mrs. Garber notes that "uniformity ... could make it impossible for a progressive locality to be a cutting edge, a vanguard, even a yardstick for the rest of the state." [128]

It is concluded, therefore, that the accuracy and security guidelines such as those recommended in Chapter V be adopted on a Statewide basis, with individual jurisdictions permitted to adopt alternate or improved guidelines if minimum standards are met. New voting systems, not previously used, should be examined for their security implications, and guidelines for their use should be adopted on a Statewide basis as part of the acceptance testing procedures.

D. The Need for Professionalization

A significant reason for the central State organization recommended by the NML is the advancement of professionalism. "A major goal in election administration should be a strong professional system that does not dilute the two-party system,"[129] it states. Mrs. Garber agrees. "I am very glad you [the NML] have chosen to make "professionalization" an important goal of election law," she comments ... "After six years in election administration, I have come to believe there is no need greater in this field than professionalization."[130] The effective use of computing technology in vote-tallying can only be enhanced by professionalization of election administration, both State and local. The computer technologists and the management technologists whose presence is required to implement the recommendations of this NBS report can only work effectively in a professional, non-partisan atmosphere.

E. The Need for Precise Terminology

One benefit of professionalization should be the adoption of more precise technical terminology in election laws and regulations, thereby making clearer the actions that must be taken in procuring, testing, and operating elections equipment. The NML report notes that election codes are "complex and ambiguous,"[131] and that local jurisdictions lack "effective guidance from the state."[132] From the viewpoint of the technologist, words like "computer" and "program" are quite ambiguous when used in regulations that should be precise in order to give specific directions. For example, does "computer" mean only the main central processing unit in which vote summation is done, or does it include all of the attached peripheral equipment? Does "computer" also include the separate and distinct small "computers" now widely used to multiplex several ballot streams onto one or more magnetic tapes for use by the main "computer"? Does "program" mean only the specific applications program for vote-tallying or does it include the supporting software such as the executive program and compiler, as well as the software of the ballot-multiplexing computers?

Regulations that concern computing technology must include definitional inputs from computing technologists. For this reason, a glossary has been included as Appendix A of this report. It is recommended that each State adopt a glossary of technical terminology to assure precise definitions, and review its regulations in that light in order to assure clarity of interpretation. Arizona[133] and Michigan[134] have begun to compile glossaries.

F. Technical Inputs to Statewide Policy Decisions

Computer technologists must not only be available on the State level to assure successful development of design specifications, glossaries,

acceptance test procedures, and to provide assistance to local jurisdictions, but they must be available to provide the technical inputs for decision making on new conditions for which no precedents exist.

Every new system has its impact on the voter in different ways. Specific voting procedures and vote-sensing methods have an inherent capability to reject or accept certain classes of questionable votes. These votes, in general, are made by voters who cannot or will not follow explicit voting instructions or who perform actions in the course of voting for which the instructions are ambiguous, uncovered, or unclear. A full understanding of the complete implications of the design of a vote-tallying system is a prerequisite for preventing the technological system from making implicit decisions that have not been consciously approved beforehand by human authority. Technical expertise is needed to provide this understanding of system implications.

Another example of a new technical condition arising for which there may be no prior experience is the transportation of ballots or the communication of ballot images outside the jurisdiction in which they were voted. Paper ballots are nearly always counted within the jurisdiction (or possibly at the county seat in which the jurisdiction is located). With voting machines, there are no ballots, and therefore no movement of ballots. But with machine-readable ballots, a reasonable proposal is to take the ballots to wherever there is a computer ready to count them (per example of Washington Township, New Jersey, section IV.B.6) or as an alternative, convert the ballots to electronic form locally and transmit them to another city, county, or State, again wherever there is a computer ready to count them.

There are clearly security implications in this problem. The movement of ballots or ballot images outside of a jurisdiction may degrade control by that jurisdiction's authorities over its election process. Movement across county lines needs to be regulated at the State level, where control can be maintained regardless of the local jurisdiction in which the ballots or ballot images are located. The movement of ballots or ballot images outside of State boundaries is also an appropriate matter for State regulation, but the awareness that problems like this exist and need control seems to require the presence of technically-trained individuals.

G. The Need for Documentation of Election Events

If modifications to existing law and regulation are to be made, and therefore any part of the entire process of public selection of office-holders is to be improved, the data required for these decisions must be available. Needed data must include documentation of difficulties that have occurred so that improvements can be factually based. At present, there are very few specifically documented reports of difficulties in local elections because in general, few requirements for such reports exist. In most cases, only when specific hearings are

initiated before courts or other administrative authorities, is any kind of first-hand reporting of difficulties available. As the League of Women Voters reports, "Where regular reports are made to a central state authority, moreover, the survey [of election practices] revealed that they generally contain no more than facts and figures regarding registration and voting rates and occasionally information on the kind of voting system used (automatic voting machines, paper ballots, etc.)."[135] Yet, the same report also states that "machine breakdown ... occurred in one out of every ten places having voting machines,"[136] a conclusion reached by the League from observations at polling places in the course of data collection for their report.

The present report has documented in Chapter IV (section IV.A.6, Harris County, Texas) an instance in which charges of "sabotage" and counter-charges of "violation ... of voting rights" were made and no State or other investigation was conducted. An investigation would have provided the evidence of a public record. Instead, the evidence of this situation (and of several other situations detailed in Chapter IV) was obtained from newspaper articles and personal conversations.

The precinct worker, whose letter to the editor published in the Washington Post, stated that "I found that the election official was ... releasing false information, [and] allowed the ballot boxes to remain unattended on the street ..." ought to have a more official place to make such complaints, simply in the interest of having these problems corrected the next time around. The editorial in the Seattle Post-Intelligencer, reported in section IV.B.5 that stated that "Many [election day workers] report they do not like to work at the polls since it is now impossible with punch cards to keep track of the ballot results as reflected against the number of persons who have signed in to vote," provides evidence, not only of personnel dissatisfaction but of possible difficulties in ballot reconciliation. The NML report concludes that "the Chief Elections Officer should therefore establish systematic procedures for receiving and hearing complaints against any election practice or official, and should make the availability of these procedures known to the public."[137]

The precinct worker is, after all, the basic operative of the voting process and the first line of defense in support of an honestly and efficiently conducted election. The ordinary voter, moreover, will be far more inclined to accept an outcome unfavorable to his chosen candidates if he or she believes that the election was conducted with strict adherence to established regulation and in an effective manner. Election administrators, many of whom are currently concerned over falling participation rates, must find ways of assuring citizens that they, the citizens, are not powerless to change the "system" when it isn't working as well as it might.

Therefore, it is recommended that immediately following each election, a public record to be filed in due course with the Chief State Elections Officer should be established and held open for a limited period of time. Each chief local elections administrator should be required to file a report in the record on the conduct of the election, specifically documenting failures of equipment and other difficulties encountered, their causes and expected solutions. In addition, voluntary, notarized statements by participants testifying to directly observed difficulties or questionable activities should be accepted into the record.

VIII. RECOMMENDED ADDITIONAL RESEARCH AND OTHER ACTIVITIES

A. Research into and Assessment of Voting Systems Technology

As was pointed out in Chapter VII, the marketplace of electronic voting systems is extremely fragmented. There is fragmentation of the sellers as well as the buyers. Failures of equipment to perform are well publicized and any large manufacturer capable of investing significant research and development funds may hesitate to make the investment due to fears of unfavorable exposure, as well as market fragmentation. This would be particularly true of a manufacturer serving a diversified clientele, for whom voting systems would be a sideline. As a result, private companies involved in newer forms of voting systems tend to be small with little capital available for extensive research. There is, therefore, no consistent direction to research, nor any concentration on those problems of research requiring the largest investment and the longest lead times before any returns can be realized.

Technical problems needing specific attention include the design of computer programs for greater intelligibility and ease of auditing and testing by the government users, the design of machine-readable ballot systems in which overvoting can be automatically prevented and chad totally eliminated, and the design of newer remote voting systems possibly involving consoles and telecommunications.

A continuous assessment of new techniques is required, in order to make known the state-of-the-art to election administrators and to insure that they will only employ proven technology that is reliable, well-engineered and economical to use. An example of new technology that has received some publicity is voting by telephone.

It was reported in Datamation, March 1974, that "the State of Washington has commissioned Pacific Northwest Bell Telephone to develop a pilot phone-a-vote system in time for a sample election, involving 2000 voters in September"...."Washington, if the test election goes well, is considering implementing 39 such systems."[138] However, in a letter to the National Bureau of Standards, dated October 3, 1974, Mr. John J. Pearson, Assistant Supervisor of Elections for the State of Washington stated that regarding the vote-by-telephone proposal, "no comprehensive paper has been written by our office dealing with the subject, as we determined from discussions with various parties that, at the present time, the proposal was both financially and physically impractical."[139] This situation is an example of one that needed to be called to the attention of election administrators, in order to prevent them from having to repeat the same investigation.

In vote-by-phone systems, voiceprints may be used in the future as voter-recognition mechanisms. At present, however, their acceptability is not universal. The U.S. Court of Appeals in Washington, D.C. ruled in 1974 that "voiceprint identification is not sufficiently accepted by the scientific community as a whole to form a basis for a

jury's determination of guilt or innocence."[140] This ruling is binding only on Federal courts in the district of Columbia circuit but, as the first Federal appellate ruling on the subject, can be expected to carry "a good deal of weight" in other Federal and State courts.[141] State courts in Florida and Minnesota now admit voiceprints but the New Jersey Supreme Court has ruled them inadmissible.[142] Further research may make voiceprinting a more certain and therefore more acceptable technique of remote voter identification.

Systems which connect to the vote-tallying system also must be considered to completely insure accuracy and security. A computer-based voter registration system impacts vote-tallying and can effect its performance. Research efforts in connecting systems are warranted.

B. Research into Human Engineering of Voting Systems

Since voting systems are used by the general public, a great majority of whom are not technically trained, it is important that these systems be specifically designed for the ease of the user. There is a lack of technical data on how individuals react to specific types of equipment, what kinds of errors they make, and in particular, how voting drop-off, that is, the tendency of voters not to vote for candidates of lower level offices, is affected by different voting systems. Ballot design, including the question of how much the first candidate listed actually benefits, if at all, deserves attention.

Research results, both into the technical aspects of system design and the human engineering aspects, would be extremely valuable for States to obtain. These results would assist States in their decision-making processes as to what systems to procure, what problems each system has, and the efforts that the States must expend in training and in technology to overcome these difficulties.

C. Improving the Transfer of Techniques

At present, there is no organized technical information collection and exchange program among election administrators. Under this situation the exchange of experiences and solutions among States and localities becomes an opportunistic and informal occurrence. This situtation inhibits State and local election administrators from obtaining the data necessary for making the best choices in specifying, testing, purchasing, and operating elections equipment. The report Power to the States-Mobilizing Public Technology, while aware of the importance of interstate technology transfer, notes its lack. "While information does migrate, it does so unevenly and fortuitously. Some of the most striking innovations by State governments are totally unknown to the others,"[143] it states.

Some of the techniques which need to be communicated are:

- successful and unsuccessful voting procedures;
- successful training tools and techniques for election workers;
- characteristics of election equipment under operating conditions;
- failures of election equipment; and
- new developments in elections technology.

The public records of elections, recommended in Chapter VII, are intended to serve as some of the data sources to satisfy election administrators' needs for information.

It is concluded that some nationwide program in the dissemination and exchange of election techniques is required to more rapidly improve election administration, to prevent redundant investigations, and to make the best use of scarce technical and administrative talent.

D. Specific State Assistance Efforts

As States begin to adopt more advanced technological equipment for election purposes, they will begin to require the kind of technical organization that can specify, procure, test, and write regulations for the use of this kind of equipment. Based on discussions and observations, it is concluded that many States may need outside assistance to help them establish this organization and commence its operation. They will need assistance in developing an organization chart and mission statement, in identifying the necessary staff competencies, in establishing the necessary testing facilities, and in writing equipment and software specifications and test criteria.

A pilot project, assisting one or two States in such an effort would be valuable. The experience of the few States that have organizations of this type, such as California, could be employed to assist in this effort. This project could then serve as a model for transfer to other States for implementation. The most cost-effective transfer would occur if the original assistance were provided under a non-proprietary arrangement. A useful output of a pilot project could include detailed procedures required to establish the organization and to develop hardware and software specifications and test criteria.

E. Capability to Audit Elections

Various observers of elections have suggested that aspects of computer-based elections be required to receive an independent review

from an outside organization. While this type of recommendation cannot be disagreed with on principle, its practicality of implementation in every jurisdiction at this time requires further investigation.

The concept of EDP auditing, of which elections auditing is a subclass, is a new one. The specific standards on which such an audit must be based have not been established, and the class of persons competent to undertake such an audit have not been delineated. It is recommended, therefore, that the subject of auditing of elections is one requiring further research. Among the aspects of this research requiring investigation are the body of information which the auditor must know, the identity of the government organization which could certify the auditor's competence to perform an EDP audit, and his specific duties with respect to an election.

F. A Federal Role

A summary of recent Federal actions in registration and voting is provided in the Council of State Governments' 1973 report Modernizing Election Systems. It notes that "Even if Congress were willing to involve the Federal government more directly in election administration, a national system would have enormous consequences for the 50 State election systems--not all of which can be anticipated--and would generate stiff resistance from State and local officials."[144] It continues, "Notwithstanding its disadvantages, a Federal system of election administration could develop if States fail to assume the initiative for insuring procedures that are uniform and convenient to the voters. Even though the administration of elections affects citizens as much as any other government concern, few States have assumed direct responsibility for implementing their own election laws or have established full-time officials to supervise elections as a State activity."..."Major responsibility now rests with more than 7000 units of local government who conduct elections today, These in turn are seriously handicapped by a general State reticence in providing money, mandating professional training, or even setting performance standards that would help keep voting opportunities uniform among their own political subdivisions."[145]

"In the end," the report continues, "the nature of Federal involvement depends on what the States themselves do." It concludes by quoting from a National Municipal League report that states "The unanswered question, of course, is whether the States and local communities will have the good sense to reform their election practices where needed. If they do not, Congress will surely be tempted to do it for them."[146]

If this attitude of the Council of State Governments is accepted, a reasonable role for the Federal government at this time is to closely observe State efforts to adopt more uniform and responsive practices which include concern for the effective use of computing technology in vote-tallying. The Federal government could take whatever actions it deems necessary if the States fail to act within a reasonable time.

An action that the Federal government could take now to assist States in their own efforts is for the Federal government to foster the establishment of a National Election Systems Standards Laboratory. This laboratory, although proposed as national in scope, need not be Federal. It would need the cooperation and approval of the States, however, to be effective. Its function would be to establish national standards for elections equipment and systems performance, and to recommend procedures that would assure the accuracy and security of vote-tallying. It could perform or provide resources to perform research of the type recommended in this chapter, i.e., research into and assessment of voting system technology and research into human engineering. It could engage in specific State assistance efforts.

The purposes of such a laboratory are consistent with a recommendation of a Council of State Governments' report previously noted, that "to the degree that State governments are willing to agree on product standards and performance criteria and combine their purchasing leverage on industry through new arrangements of a multi-state or regional character, industry's readiness to respond with technological innovation will be decidedly better."[121]

IX. SUMMARY GUIDELINES FOR ACCURACY AND SECURITY

A. Aids to Audit of Calculations

1. Precinct Ballot Reconciliations

The following equalities should be able to be demonstrated as part of the officially reported election results:

For each precinct and for each type of ballot used, the number of voters receiving non-absentee ballots must equal the sum of the number of non-absentee ballots counted.

For each type of ballot used excluding absentee ballots, the number of ballots distributed to each precinct must equal the sum of the number of ballot returned in all categories of use: voted unchallenged, voted challenged, spoiled, and unused.

2. Absentee Ballot Reconciliation

As part of the official election results, the number of absentee ballots distributed, the number returned for counting, and the number unreturned must be reported.

3. Overall Ballot Reconciliations

The following equalities should be able to be demonstrated as part of the officially reported election results:

For the entire election, and for each type of ballot used in it, the total number of non-absentee ballots distributed to voters must equal the number of non-absentee ballots actually counted.

For the entire election, and for each type of ballot used in the election, the total ordered to be printed must equal the sum of the number of ballots machine-counted, hand-counted, successfully challenged, spoiled, unused, and unreturned from absentee distribution.

4. Vote Count/Ballot Reconciliations

The following equalities should be able to be demonstrated for machine-counted ballots as part of the officially reported election results:

For each precinct and for each individual race in which no more than one vote may be cast by a voter, the number of non-overvoted ballots must equal the sum of counted votes for all choices in the race plus the sum of all blank ballots (no votes) for that particular race. The number of non-overvoted ballots is the difference between the total number of ballots counted and the number of overvoted ballots in that particular race.

For each precinct and for each individual race in which no more than N votes may be cast by a voter (N is an integer greater than one), N times the number of non-overvoted ballots must equal the sum of counted votes for all choices in the race plus the sum of all undervotes in the race. The number of undervotes on any ballot for a particular race is N minus the number of actual votes cast when that difference is a non-negative number.

5. Verification of District-Wide Summations

For easier verification by inspection of the summation of precinct totals to yield district-wide totals for each choice in a race, official results can include the sequence of increasing partial totals, showing the addition of each precinct's results separately into the previous partial sum.

6. Recounting

Further confidence in the machine-counted results can be achieved if mandatory machine-recounting of a percentage of the precincts voting for each race is carried out on a different, independently-managed computing system than that used to produce the official count.

The machine used for recounting may be that held available as a back-up system. If this is the case, it will have been previously checked out and ready.

The percent of total precincts required to be machine-recounted for each race should increase towards 100% as the vote totals of the opposing candidates or choices approach equality. Selection of some of the precincts for recounting should be granted to candidates and to official proposition and referendum supporters and opponents. Mandatory small-sample manual recounting should also be carried out.

B. Effective Control of Ballots and Computer Hard-Copy Records

1. Precinct Ballot Control

Control over ballots for reconciliation purposes will be simplified if each ballot has two stubs, numbered identically but uniquely with respect to all other ballots of the same type. The outer stubs of each ballot of groups of one-hundred or multiples of one-hundred ballots can be stapled together to a backing for easy handling, distribution, and counting.

At a voting location, a voter can be given a ballot still attached to the inner stub, leaving the outer stub with precinct officials. Following the marking or punching of the ballot by the voter, but before the ballot is deposited, the number on the inner stub is compared for a match against the number of the outer stub recorded as being given the voter. At this time, the voter's ballot choices must be protected

by an envelope. The stub numbers must match for the voter to be permitted to deposit his ballot. The inner stub is separated before the ballot is deposited in the ballot box or entered into a ballot summarizer, whichever is being used in the precinct.

2. Absentee Ballot Control

Absentee ballots can be controlled like non-absentee ballots (as described above), if each absentee voter is given or mailed a ballot with its inner stub attached. An example of a control procedure is as follows. The absentee voter can be provided with two envelopes, an inner one for the ballot and an outer one for the stub. The voter should be instructed to remove the stub and to seal just the ballot in the inner envelope. The stub is mailed back in the outer envelope. As each outer envelope is opened, the returned inner stub is matched against the outer stub retained by the election officials. Following the match, the inner envelope is physically separated from the stub and outer envelope and mixed with other absentee ballots similarly separated so that all relationship of the ballot and its identifying stub is destroyed. The absentee voter must be instructed not to make any marks on the inner envelope.

3. Machine Readability of Ballots' Precinct Number

Each ballot should be identified as to precinct and type of ballot in both a human readable and machine-readable form.

4. Control of Header Materials Used In Computing Devices

The blank stock from which header materials such as cards or punched tapes are obtained should be controlled in quantity and visually distinct. Each card or tape segment should have an inventory control number associated with it for accounting purposes. These materials should be treated like official election records.

5. Output Listing of Header Materials

Header materials used in the course of vote-tallying should be listed unmodified on the output printer of the computing device into which they are inserted in order to verify their exact content.

6. Control of Computer Output Hard Copy

Cards or perforated tapes that are punched to contain partial results of election totals should be initially obtained from blank stock that is controlled in quantity and visually distinct. An inventory control number should be associated with each card or tape segment for accounting purposes. Computer output printer paper, when used for the same purposes, should be similarly treated.

7. Verification of Candidate Rotation

Candidates should be listed on the computer output report for each individual precinct in the same rotational order as they were listed on the voting instructional materials for that precinct.

C. Security of Computer Programs and Systems

1. Use of Dedicated Operation

A computing system dedicated only to vote-tallying, while vote-tallying programs are being tested or run, is preferred and more secure than any other arrangement of computer use.

2. Initialization of System

Before beginning vote-tallying program testing or running on a computer also used for other purposes, all extraneous peripheral equipment should be physically disconnected. The erasure of memory locations that are to remain accessible to the system, except those minimally required to load a new operating system, if any, should be accomplished. Active measures should be undertaken to assure that all tapes and discs to be used that are supposed to be initially blank are actually blank (except for machine-readable inventory identifiers) and have no defects.

3. Procurement of Support Software

Separate copies of all computer support software should be obtained from a general supplier from his stock of standard products; or should be written in-house. Demonstration by the supplier, through bit-for-bit comparison, that the copies received are standard products, unaltered in any way, is desirable. Listings should be secured for future reference.

4. Use of Minimum Complexity

The least complex support software that provides the capabilities required by vote-tallying should be employed.

5. Use of Dedicated Support Software

All the support software used with vote-tallying programs should be maintained on media under the control of the election administration and not used for any other purpose.

6. Physical Protection of Object Codes

Master copies of all programs, including support software and application programs, should be retained in secured locations,

separate from the location of working copies. The master copy, once generated, is always used in a read-only mode. No writing is ever done on the storage medium of the master copy.

Before use of the working copy it should be compared, bit-for-bit against the master copy. Any differences must be explainable. When running an election, a reasonable procedure is to require a bit-for-bit comparison of all software used against master copies immediately before and immediately after ballot counting.

7. Simplified Control For Comparisons and Regeneration

When any comparison of copies is done, the computer should be under the control of the most elementary kind of supervisory program whose logic is obvious by inspection and whose sole function is this comparison. If it is ever necessary to generate a working copy from a master copy, or to regenerate a master copy, a similar elementary supervisory program should be employed.

8. Programmatic Protection of Object Codes

Listings taken from software can be used to assure that key instructions remain in their known relative locations and that the size of object code remains fixed.

Other protective techniques that can be employed require some program alteration. A program can be provided with a parameter that indicates how many times the program has been run. This number should match with a corresponding log book entry. A program can also be provided with a set of parameters which will prevent further execution of the program unless a data card containing matching parameters known to a minimum of persons is entered. Redundant code can be added to a program that checks the calculations performed along a parallel path.

9. Labeling of Discs and Tapes

Discs and tapes employed for any vote-tallying purpose should have both human-readable and machine-readable labels. When the machine-readable label is read by the operating system, a halt in further operation should occur until the computer operator enters the human-readable label. A match between the two labels must precede any further computer operation.

10. Control of System Control Cards

Punched cards, used for modification of operating system conditions should have a use code and version number punched in identification fields of the cards. Each card should be checked for proper use and version when read by the operating system and the effect of the card on system operation reported on the system output printer.

11. Logging of Operations

The operating system of the computer must be programmed to report automatically on the system printer all actions taken by the operators to change conditions, and their times of occurrence.

The operators themselves must report in a log book all significant actions they have taken with respect to altering computer operations in any way, and the times of occurrence. These actions will include mounting and dismounting tapes, connecting or removing peripherals, insertion of data, or changing of control switch settings.

12. Separation of Computer Room Duties

A basic principle of internal control is to divide the execution of critical functions between two or more persons. One individual should never be totally responsible for a given activity, such as computer operation or program development.

13. Control of Program Changes

Every change to a computer program, even those involving only one statement, should be authorized, approved, and documented with no exceptions.

D. Use of Teleprocessing

1. Accuracy and Security Protection

Vote-tallying data must be protected during teleprocessing against inaccuracy due to electrical noise, and against unauthorized interception or alteration. Alteration may involve deletion of correct data and/or insertion of false data.

2. Transmission Before Close of Polls

Where public knowledge of voting results before the polls are closed is unlawful, transmission of voted ballot data or summaried results while the polls are open must be protected from interception.

3. Use of Synchronous Transmission

Synchronous transmission is inherently less vulnerable to interception or alteration than asynchronous transmission since greater knowledge of block structure and control procedures would be required.

4. Use of Checksum Polynomials

In teleprocessing of vote data, a cyclic redundancy checksum polynomial for error detection purposes should be appended to each block of data transmitted. The polynomials known by the abbreviations CCITT

and CRC-16 are among those acceptable. The CCITT polynomial has the status of an international standard and is recommended.

5. Use of Encryption to Prevent Interception

Encryption is a technique that may be used to prevent interception. The situation most demanding of the use of encryption is that in which personal identification of the voter is transmitted with the voter's choices. Another situation in which encryption is warranted is transmission before the polls are closed of voting results summarized at the precinct level or higher. Encryption is worthy of consideration if individual ballot data, not personally identified, is transmitted before the polls are closed.

6. Use of Encryption to Prevent Alteration

If encryption is not used in the teleprocessing of vote data, there is a possibility that a sophisticated disrupter could delete correct data or replace correct data with false data on the line. Encryption can be used to guard against this threat.

7. Retention and Verification of Transmitted Copy

To eliminate any permanent effect due to inaccuracy or deliberate alteration of transmitted data, a copy of the data sent should be retained at the transmitting end in an easily machine-readable form, e.g. magnetic tape. Then, verification of the data transmitted can be easily carried out following a transportation of the tape to the computing site.

E. Design Specifications for Vote-Tallying Computer Programs

1. Use of High-Level Language

To maximize clarity, a high-level language such as COBOL is preferred for use in writing any vote-tallying program meant to be executed on a stored-program, general-purpose computer.

2. Documentation

Listings, flow charts, and program comments provide further clarity and are needed to assure effective examinations of a program during acceptance testing.

3. Use of Table-Driven Code

A program design is preferred which allows the program to retain its basic logic structure when altered for use in different elections. Table-driven code provides this capability.

4. Use of Modularity

Modular program design is preferred. This form of design subdivides the program into separate, smaller, self-contained units making the program more easily subject to analysis. Each module has well-defined input and output functions and single entry and exit points. Testing of each module separately is possible.

5. Inclusion of Audit Trails

Program design should allow for inclusion of audit trails of calculations. The design should include the capabilities of: providing the number of ballots machine-counted for each precinct, providing the partial sum of district-wide official totals following the addition of each individual precinct's results into those totals, reading the precinct number from each ballot and checking for that number's correctness, providing the number of overvotes and undervotes for each office in each precinct, copying out on the output printer the exact contents of each header and control card read at the input, and reading out the list of candidates for each office in each precinct's summary report in the same rotational sequence that they were listed in the instructional materials for that precinct.

6. Provisions for Testing

A vote-tallying program should be capable of receiving inputs of ballot images on tape or disc to permit testing of the program against a large number of simulated votes.

F. Acceptance Testing of Vote-Tallying Programs

1. Function

Acceptance testing is a separate process preceding pre-election checkout. It must include a demonstration that imposed design specifications have been met.

2. Use of Realistic Conditions

Conditions under which a vote-tallying program will be used in any election for which it is approved should be employed or simulated during testing. This will involve testing the program for its maximum capabilities. These capabilities include, for example, the various combinations of offices, candidates, precincts, and ballot configurations that the program is capable of handling. The program should be tested on each distinctive hardware and support software combination with which it is designed to run. A full simulation of the largest number of ballots expected to be handled by the program should be carried out. Simulated ballots should include those that are designed to test the program's logical ability to deal correctly with expected as well as unusual combinations of voting patterns.

3. Ballot-Image Generating Program

A computer program needs to be available which has as its function the generation of a large number of ballots or ballot images that sum to pre-determined results. The purpose of this program is for testing a vote-tallying program against a full complement of votes. The program should be capable of generating ballots or ballot images with various combinations of overvoted and non-overvoted offices in each precinct and should have the capability of simulating the use of unassigned ballot locations.

G. Design Specifications for Election Equipment and Supplies

1. Need for Specifications

Imposition of design specifications for both simple and complex equipment and supplies is an important management tool that ought to be employed to its fullest capability.

2. Sensor Specifications

The sensor, the device which converts information on a ballot to electronic form for data processing, is one of the key elements of a computer-based vote-tallying system. Its accuracy, reliability, and stability over time must be assured.

3. Coordination of Sensor and Other Specifications

Coordination of design specifications among the ballot, vote-encoding equipment and the sensor are of paramount importance to overall vote-tallying system accuracy. Sensor accuracy must be considered in combination with the quality of its data input which voters are able to achieve given particular forms of ballots and vote-encoding equipment.

4. Sensor Effect on Ballots

The effect of a sensor on the information contained on a ballot must be minimal when the ballot is read. This is extremely important if a ballot must be re-read or recounted.

5. General Equipment and Supply Specifications

Specifications which can be imposed on equipment and supplies include operability under varying environmental conditions, mean times to repair and mean times to failure, availability of spare parts (both short term and long term), availability of maintenance assistance, and durability in transport and while being used by voters, if applicable.

6. Design Specifications for Summarizers

Audit trails of calculations are needed for ballot and vote

summarizers as they are needed in vote-tallying computer programs meant to run on general-purpose, stored program computers. With summarizers, the equivalent audit trails may have to be implemented in hardware. In these cases, design specifications will need to be imposed on the summarizer equipment to achieve the necessary audit trails.

H. Acceptance Testing of Vote-Tallying Equipment

1. Concept and Complexity of Testing

The concept of acceptance testing implies that there exists a group of identical devices and that some subset of these are to undergo specific tests determining whether design specifications are met. If those undergoing tests pass, then it is assumed that the remainder, designed identically, also would have passed the same tests. Selection of the subset chosen to be tested and the complexity of the tests imposed depend on the absolute size of the set, the expected variability of test parameters in manufacturing, and the criticality of the operating parameters of the items for successful operation of the system of which they are a part.

2. Acceptance Testing of Sensor Equipment

The sensor may be tested first against an "ideal" ballot, one providing maximum difference between a vote and no vote. The sensor must, in addition, be tested in combination with the ballot and vote-encoding equipment under simulated actual conditions to determine if this important subsystem meets acceptable accuracy standards. A statistical sample of voters should be employed for this test.

3. Output of Acceptance Test

A major output of a successful acceptance test should be a document communicated to those persons who will perform pre-election checkout. This document should describe how each approved device is to be demonstrated to be working acceptably.

I. Pre-Election Checkout of Vote-Tallying Systems

1. Waiting Period Following Initial Acceptance

The first use of election hardware or software in an election should not be permitted until several months after the hardware or software has passed its acceptance test. The purpose of this waiting period is to insure that a jurisdiction is not committed to an unacceptable system and has sufficient time to select an alternate system. Experimental tests of systems on a small scale can be excepted from this rule.

2. Full-Scale Checkout

To the greatest extent possible, all hardware and software to be utilized should be given a dry run simulating specific conditions to be faced on election day and election night.

3. Personnel Activities Checkout

A full-scale dry run must, of necessity, involve many elections personnel. This will help operational personnel to be more sure of their duties.

4. Contingency Plans and Back-Up Equipment

Pre-election plans must consider situations which will not go as initially expected. Spare personnel, parts, and supplies must be held in readiness at locations where phone communications are available and sufficient for emergency conditions. Contingency procedures for all failures that can be anticipated, e.g. card reader jams, should be developed.

Failure of centralized computing equipment must be considered a possibility and alternate sites held in readiness. The readiness of a back-up site may provide the capability for machine-recounting, previously discussed.

5. Documentation of Summarizer Alterations

If ballot or vote-summarizers are used in an election instead of, or in addition to, general purpose computers, they will have to be specialized for the particular election. As part of the pre-election checkout, documentation procedures must be established to record and control the changes that are made to summarizers to specialize them. This documentation must become part of the official election records.

J. Assurance of Management Control

1. Control of Resources

The chief local elections administrator must have full management control over all resources (personnel, equipment, supplies, and sites) employed during the voting and vote-tallying process until such control is voluntarily relinquished when no longer needed.

2. Vendor Responsibilities

Procedures which explicitly delineate the responsibilities of vendors of equipment, supplies and services must be worked out in advance. Each vendor should have his own checkout procedures; and he should document the checkout activities specifically undertaken before

the equipment, supplies, and/or personnel are turned over to the administration's control for election purposes.

3. Transfer of Control

Procedures, including documentation, covering the transfer of control of equipment back to any vendor for repairs, if necessary during the voting or vote-tallying process, should be pre-arranged. While equipment is under vendor control, no operational election activities should be carried out, as all of these must be under the control of the election administration.

Appendix A: GLOSSARY OF TECHNICAL TERMS

The following definitions pertain to this report and are not intended to be taken as standards. However, some of the definitions are in accordance with the publication American National Standard Vocabulary for Information Processing, ANSI X3.12-1970, published by the American National Standards Institute, Inc. These definitions are marked "ANS."

Other definitions have been adopted from the latest draft of the American National Dictionary for Information Processing, which is expected to be published by the American National Standards Institute, Inc. in 1975. This publication will supersede X3.12-1970. Definitions below which are in accord with the current draft are marked "DIP."

Definitions which are in accord with both X3.12-1970 and the draft Dictionary are marked "ANS/DIP." Other definitions adopted solely for this report are marked "R." Words that are the subject of definitions are underlined in the definitions below.

application program

(R) A computer program that solves a problem posed by a computer user. Contrast with support software.

assembly language

(R) A computer-oriented language whose instructions are usually in one-to-one correspondence with machine instructions.

asynchronous transmission

(R) Teleprocessing of a sequence of characters occurring without a predicted time relationship among them. Contrast with synchronous transmission.

ballot holder

(R) A device used to hold a ballot in a fixed position in preparation for punching by a voter.

ballot image

(R) A corresponding representation in electronic form of the punch or mark pattern of a voted ballot.

ballot style

(R) One of the several formats of a ballot issued equivalently in different precincts. Contrast with ballot type.

ballot summarizer

(R) A special-purpose computing device integrated with a sensor which accepts ballots and tallies them. Contrast vote summarizer.

ballot type

(R) One of the individual kinds of ballots containing distinctly different offices or issues given together to a single voter. Contrast with ballot style.

bit

(R) Synonymous with binary digit. A digit which can take on only one of two possible values, usually either 0 or 1.

block

(R) A string of characters or bytes treated as a logical entity.

bug

(ANS/DIP) A mistake or malfunction.

byte

(ANS) A sequence of adjacent binary digits operated upon as a unit and usually shorter than a computer word.

central processing unit

(ANS/DIP) A unit of a computer that includes the circuits controlling the interpretation and execution of instructions. Synonymous with main frame. Abbreviated CPU.

chad

(ANS) The piece of material removed when forming a hole or notch in a storage medium such as punched tape or punched cards. Synonymous with chip.

character

(ANS) A letter, digit, or other symbol that is used as part of the organization, control, or representation of data. A character is often in the form of a spatial arrangement of adjacent or connected strokes.

checksum polynomial

(R) A sequence of bits appended to the end of a transmitted block

of data for the purpose of detecting an error in transmission of the block.

COBOL

(ANS) (COmmon Business Oriented Language). A business data processing language.

(R) An example of a high-level language and a problem-oriented language.

comment

(DIP) A description, reference, or explanation, added to or interspersed among the statements of the source language that has no effect in the target language.

compiler

(R) A computer program employed to translate another computer program expressed in a problem-oriented language into object code.

computer

(ANS) A data processor that can perform substantial computation, including numerous arithmetic or logical operations, without intervention by a human operator during the run.

computer program

(ANS) A series of instructions or statements, in a form acceptable to a computer, prepared in order to achieve a certain result.

computer word

(ANS) A sequence of bits or characters treated as a unit and capable of being stored in one computer location. Synonymous with machine word.

data link

(DIP) The physical means of connecting one location to another for the purpose of transmitting and receiving data.

data processor

(ANS) A device capable of performing data processing, including desk calculators, punched card machines, and computers.

decryption

(R) The inverse of encryption.

dedicated operation

(R) Devoting all resources of a computer to the execution of a single application program.

digital computer

(ANS) (1) A computer in which discrete representation of data is mainly used. (2) A computer that operates on discrete data by performing arithmetic and logic processes on these data.

disc

see magnetic disc.

encryption

(R) A process of converting a sequence of characters into another sequence by means of a private algorithm for the purpose of protecting the original sequence from unauthorized comprehension.

execution

(DIP) The process of carrying out the instructions of a computer program by a computer.

flowchart

(ANS) A graphical representation for the definition, analysis, or solution of a problem, in which symbols are used to represent operations, data, flow, equipment, etc.

frequency spectrum

(R) The set of magnitudes of vibrational components distinguishing a particular emission or signal.

general-purpose computer

(DIP) A computer that is designed to operate upon a wide variety of problems.

hard copy

(R) A storage medium in which the data is visible and non-volatile, e.g. paper or cardboard products containing printed, punched, or marked data.

hardware

(DIP) Physical equipment used in data processing, as opposed to

computer programs, procedures, rules, and associated documentation. Contrast with software.

header card

(ANS/DIP) A card that contains information related to the data in cards that follow.

high-level language

(DIP) A programming language that does not reflect the structure of any one given computer or that of any given class of computers.

(R) A programming language designed so as not to require substantial knowledge by the programmer of the internal structure of the stored-program computer on which a program written in that language is to be executed.

instruction

(DIP) In a programming language a meaningful expression that specifies one operation and identifies its operands, if any.

interactive operation

(R) A mode of operation of a digital computer in which the user of a terminal carries on a dialogue with the computer such that each unit of input entered by the user evokes a prompt response from the computer.

interception

(R) surreptitious obtainment of the contents of a message during transmission of the message.

internal storage

(ANS) Addressable storage directly controlled by the central processing unit of a digital computer.

jump

(DIP) In the execution of a computer program, a departure from the implicit or declared order in which instructions are being executed.

language

see programming language.

loop

(DIP) A set of instructions that may be executed repeatedly while

a certain condition prevails. In some implementations, no test is made to discover whether the condition prevails until the loop has been executed.

looping

(R) A condition of a computer program in which a particular sequence of instructions is being repeatedly executed. Sometimes an error condition, particularly when continued long enough to be discernable by human observation.

machine code

(R) A sequence of machine instructions.

machine instruction

(DIP) Synonym for computer instruction. An instruction that can be recognized by the central processing unit of the computer for which it is designed.

machine readable

(R) Capable of being introduced as information into a computing device.

magnetic disc

(ANS) A flat circular plate with a magnetic surface on which data can be stored by selective magnetization of portions of the flat surface.

magnetic tape

(ANS) A tape with a magnetic surface on which data can be stored by selective polarization of portions of the surface.

mark-sensing

(R) Converting a mark on a ballot produced by a voter to an equivalent electrical or electronic signal.

medium

(ANS) The material, or configuration thereof, on which data are recorded, e.g. paper tape, cards, magnetic tape. Synonymous with data medium.

memory

(ANS) Same as storage.

minicomputer

(R) A stored-program computer of relatively small size and low cost with limited facilities in some functional areas such as storage, support software, and number of input-output channels.

modularity

(R) A quality ascribed to a computer program when it is constructed of modules.

modular programming

(R) Designing and writing computer programs using the concept of modularity.

module

(R) A collection of computer program statements which can be grouped together such that the functions of input and output are well-defined, there is a single entry and a single exit point, and the exit returns control to the point from which the module was executed.

multiprogramming

(ANS) Pertaining to the concurrent execution of two or more computer programs by a computer.

non-volatile storage

(DIP) A storage whose content is not lost when the power is removed.

object code

(ANS/DIP) Output from a compiler or assembler which is itself executable machine code or is suitable for processing to produce executable machine code.

online

(ANS/DIP) (1) Pertaining to equipment or devices under control of the central processing unit. (2) Pertaining to a user's ability to interact with a computer.

operating system

(DIP) Software that controls the execution of computer programs and that may provide scheduling, debugging, input-output control, accounting, compilation, storage assignment, data management, and related services.

peripheral equipment

(DIP) In a data processing system, any equipment, distinct from the central processing unit, that may provide the system with outside communication or additional facilities.

perforated tape

see punched tape.

porta-punch card

(R) A card with prescored punch positions that can be perforated manually.

problem-oriented language

(ANS) A programming language designed for the convenient expression of a given class of problems.

programmable

(R) A quality ascribed to a device which is initially designed and constructed so that its logic of operation can be altered at a later time in a non-destructive manner.

programming language

(DIP) An artificial language established for expressing computer programs.

punched tape

(ANS) A tape on which a pattern of holes or cuts is used to represent data.

read-only memory

(R) A memory designed so that, during operation, data can be retrieved from it but not entered into it.

remote access

(DIP) Pertaining to communication with a data processing facility through a data link.

routine

(ANS/DIP) An ordered set of instructions that may have some general or frequent use.

security

(R) Protection of hardware, software, and data through the imposition of appropriate safeguards.

sensor

(R) In vote-tallying, a device which responds to the presence of a mark or punch on a ballot by producing an equivalent electrical or electronic signal.

software

(DIP) Computer programs, procedures, rules, and possibly associated documentation concerned with the operation of a data processing system. Contrast with hardware.

source language

(R) The programming language other than machine code, in which a computer program is written and from which the program is translated to obtain machine code.

source program

(DIP) A computer program expressed in a source language.

statement

(DIP) In a programming language, a meaningful expression that may describe or specify operations and is complete in the context of this programming language. (Contrast with comment.)

storage

(ANS) Pertaining to a device into which data can be entered, in which they can be held, and from which they can be retrieved at a later time.

storage medium

see medium.

stored-program computer

(DIP) A computer controlled by internally stored instructions, that can synthesize and store instructions, and that can subsequently execute these instructions. Synonymous with programmed computer.

stylus

(R) In voting, a hand-held pointed object used for punching out pre-scored locations on a porta-punch card.

supervisory program

(ANS/DIP) A computer program, usually part of an operating system, that controls the execution of other computer programs and regulates the flow of work in a data processing system. Synonymous with executive program, supervisor.

support software

(R) All software, such as an operating system, that does not pertain to any specific application or application program.

synchronous transmission

(R) Teleprocessing a sequence of characters or bytes as a block, at a fixed rate of transmission over the length of the block.

system control card

(R) A punched card used for the purpose of changing the state of an operating system or supervisory program.

table-driven program

(R) A computer program designed such that all the parameters which distinguish a particular execution of the program from any other execution may be found in a set of tables contained in the program.

tape

see magnetic tape, punched tape.

target language

(DIP) A language into which statements are translated. Synonymous with object language.

teleprocessing

(R) The use of telecommunications facilities for the transmission of data to or from a data processor.

terminal

(ANS/DIP) A point in a system or communication network at which data can either enter or leave.

vote summarizer

(R) A special-purpose computing device on which voters select their choices directly and which tallies each voter's choices as they are finalized with the choices of all previous voters. Contrast with ballot summarizer.

Appendix B: MATHEMATICAL CONSIDERATIONS AND IMPLICATIONS IN SELECTION OF RECOUNT QUANTITIES

One attribute of machine-readable ballots is that it is possible to recount them by a second method, either by manually recounting them or by machine-recounting them on a different, independently-managed computer system. After some difficulties with machine-readable balloting had occurred in California, that state decreed that a manual recount of 1% of all precincts, but in no case less than six precincts, must be undertaken in each election in which machine counting was used. A question may then be asked about the reasonableness of the number "1%". Under what conditions does a "1%" recount constitute a satisfactory check, and under what conditions is it less satisfactory?

More generally, what quantity of recount under what conditions will give a high confidence level that the originally reported results of the election are entirely correct? If the recounted portion agrees completely with the original report for those precincts, it will be assumed that those precincts not recounted are also correct as originally reported. If the recounted portion differs substantially from what was originally reported, a simple decision rule could be that all remaining ballots must be recounted. Other decision rules, mathematically based, could be devised, based on actual differences between the original and recounted values, but are not considered here. It can be reasonably assumed that once any significant difference is demonstrated between supposedly equal quantities, as a practical matter political rather than mathematical considerations will be overriding.

1. An Example

To investigate the question of the proper partial recount quantity in more detail, consider the following simplified example. Suppose, in a certain jurisdiction, there were exactly 1,000 precincts, and in an election just concluded, exactly 1,000 persons voted in each precinct. Suppose also that there were just two opposing candidates and there were no overvotes or undervotes. In addition, suppose the final tally originally reported was 505,000 to 495,000, a difference of 1%, or 10,000 votes out of 1,000,000 cast.

Now, to cause a reversal in outcome, there must be a vote-switch of more than 5,000 votes, but this is only 1/2% of all votes cast. This misreporting could be accomplished in any of several ways:

(a) by a switch of a minimum of 5 votes in each of the 1,000 precincts;

(b) by a switch of a minimum of 50 votes in each of 100 precincts;

(c) by a switch of a minimum of 500 votes in 10 precincts; or

(d) by a switch of some intermediate product of precincts and votes per precinct, still switching a total of 5,000 or more votes.

The above possibilities consider only vote-switching schemes in which the total vote for both candidates remains the same. There are, of course, an infinite set of possible incorrect outcomes that could be reported, but only those which involve a direct switch from one candidate to the other will retain the total vote constant. It is assumed that ballot and vote reconciliations are made as a matter of standard practice, so that any reporting error which does not retain the constancy of the total vote cast can be discovered in that manner.

Note, however, that a vote-switch using the schema of (a) above would be caught immediately if any single precinct were recounted, regardless of which one were chosen. Thus, this schema is not a likely one for a vote switching error to get by unnoticed. Similarly, the schema of (c) would clearly be observed by the opposition by a simple inspection of the results reported, since it requires a switching of 50% of the vote in a limited number of precincts. An alert opposition would demand a recount in these specific precincts.

Suppose, however, that a vote-switch using the schema (b) actually occurred. This requires a switch of only 5% of the vote per precinct in only 100, or 10% of the precincts. Now it is not clear that an alert opposition could spot by inspection those precincts in which misreporting had occurred and could pick out the proper precincts for which to demand a recount.

In this case, there may be errors in some of the precinct results, but the specific precincts cannot be determined by inspection or by a minimum recount. Specific precincts are therefore randomly chosen to be recounted and hopefully, one in which misreporting (vote-switching) has occurred will be chosen. If no vote-switch precincts are chosen for recount, the error will go undetected, if there is any. The error is considered detected if at least one misreported precinct is selected for recount.

Consider the 1% rule applied to this problem. Just ten of the 1,000 precincts are chosen to be recounted and we want to determine the probability that one of the ten chosen for recount will be one of the one hundred in which vote-switching has occurred.

Let P be the probability that at least one precinct chosen for recount has been misreported. Thus P is the probability of detecting the vote-switch. Then $1 - P = \bar{P}$ is the probability that all precincts chosen for recounting have been correctly reported. The probability that the first precinct chosen is correctly reported is 900/1000. Given that the first precinct chosen is correctly reported, the probability that the second precinct chosen is correctly reported is 899/999. Given that the previous nine precincts chosen were correctly reported, the probability that the tenth chosen is also correctly reported is 891/991.

Thus, the probability that all chosen are correctly reported is:

$$\bar{P} = \left(\frac{900}{1000}\right) \cdot \left(\frac{899}{999}\right) \cdot \left(\frac{898}{998}\right) \cdot \cdots \left(\frac{891}{991}\right)$$

or $\bar{P} = .345$

or $P = 1 - \bar{P} = .655$

The probability of discovering the vote switch by recounting 10 precincts is .655. The number .655 indicates that if there were many situations of exactly this type with the parameters of this problem, only about 2 out of 3 of them would be discovered, using a one percent recount. Many persons concerned with elections may find this fraction unacceptably low. The acceptably fraction may be at least .9, possibly .99, if not .999.

In this example, with 1,000 precincts and 100 of them misreported, it would take a recount of 22 precincts (2.2%) to assure a 0.9 probability of choosing for recounting at least one of the misreported. It would take a recount of 43 precincts (4.3%) to assure a probability of 0.99, and it would take 64 precincts (6.4%) to assure more than a 0.999 probability of choosing for recounting one of the misreported. To assure an absolute certainty (1.000 probability) of selecting at least one misreported precinct would require a recount of 901 precincts or 90.1% of all precincts. There is a certain efficiency, therefore, in not demanding an absolute certainty.

2. Undetectability by Observation

An important parameter determining the partial recount quantity is the maximum level of undetectability by observation. This is the largest percent switch of votes in any one precinct that will fail to make the opposition correctly suspicious that a switch has occurred in that precinct. The higher the maximum level of undetectability by observation, the higher the number of switched votes that can be packed into a single precinct, and the fewer the number of misreported precincts that are needed to reverse an election. The fewer the number of misreported precincts needed to reverse an election, the less likelihood there is of a vote-switching scheme being discovered by a partial recount. As a consequence, a higher level of undetectability by observation implies a larger partial recount quantity.

If the maximum level of undetectability by observation were 5% of the vote per precinct then, in the example above, the schema (b) would minimize the number of misreported precincts that could reverse an election. No other schema would minimize the probability of detection in this example. If less than 5% of the vote per precinct were switched, more than the minimum number of precincts would need to be misreported and the probability of discovery in a partial recount would be increased. If more than 5% of the votes in a precinct were switched, these results

would be obvious to the opposition (by definition) and discovery by observation would occur.

It follows that an alert political party will keep good records of each precinct's voting patterns historically and with respect to similar precincts in the same election, thus minimizing the maximum level of undetectability by observation. The actual numerical value of this level may vary from jurisdiction to jurisdiction or even from precinct to precinct, and it is a problem for political scientists and election administrators to select the actual values.

It may be that a reasonable value is in the neighborhood of 5% to 10%. That is, a 5% maximum level means that a true 50%-50% vote split could be switched to 55%-45% (or a 52.5%-47.5% vote could be reversed) without arousing suspicion; and a 10% maximum level means that a true 50%-50% vote split could be switched to 60%-40% (or a 55%-45% vote could be reversed) without arousing suspicion.

3. Development of a General Recount Formula

Consider now the development of a general formula to determine the necessary partial recount quantity to assure a particular probability of detection of misreporting based on a given maximum level of undetectability by observation.

As before, let P equal the desired and given probability that a partial recount will select for recounting at least one vote-switched precinct. The value of P also, whether 0.9, 0.99, 0.999, or some other value, must be selected by subjective decision since it depends on the trade-off between effort expended on recount and confidence that the true voted results are mirrored in the published figures.

Then, as before $1 - P = \bar{P}$ is the probability that no misreported precincts will be selected for recounting.

Let p equal the total number of precincts; f equal the number of misreported precincts; and r equal the number of precincts recounted. Then, by analogy with the example above:

$$\bar{P} \geqslant \prod_{k=0}^{r-1} \left(\frac{p-f-k}{p-k} \right) \qquad (1)$$

Equation (1) is essentially a formula for independent sampling without replacement. The precincts being recounted are the samples. The probability of the first sampled precinct being correctly reported is (p-f)/p and sampling of precincts for recounting continues until that value of r is reached at which the cumulative probability of selecting only correctly-reported precincts is equal to or less than the given $\bar{P}$. An inequality is shown in (1) because it is assumed that $\bar{P}$ is known in advance and the problem is to find r, the number of precincts to be

recounted. As r must be an integer, it is unlikely that the right-hand product in (1) will equal the given $\bar{P}$ exactly.

Now, solving for P,

$$P \leq 1 - \prod_{k=0}^{r-1} \left(\frac{p-f-k}{p-k}\right) \qquad (2)$$

If x, the maximum level of undetectability by observation is given as a fraction, and d, the difference in the candidates' votes plus one (in a two-candidate race) is also given, then f, the minimum number of vote-switched precincts that will overturn the contest is easily computed.

First, d/2 (plus 1/2 if d is odd) is the minimum number of votes that must be switched in order to reverse the election, and let n be the total number of votes cast. Then, n/p is the number of votes per precinct, (assuming an equal number of votes in each precinct) and nx/p is the maximum number of votes in each precinct that can be switched without detection by observation. Then the minimum number of vote-switched precincts required to reverse the election is:

$$f = \frac{d/2}{nx/p} = \frac{p}{x} \cdot \frac{d}{2n} \qquad (3)$$

In (3), d/n is the fractional difference between the candidates and d/2n is the minimum fractional difference between the candidates that needs to be switched in order to reverse the election. As f must be an integer number of precincts, if it is not as a result of calculation from (3), the next highest integer is selected.

By substituting (3) for f into (2), the number of precincts to be recounted, r, is determined as a function of P, p, x, and d/2n. Of these independent variables, P, p, and x are determined independently of the election results and d/2n is established directly as a result of the originally-reported tally.

Tables 1, 2 and 3 show the results of calculations on equation (2), with (3) substituted for f, for values of P, the probability of selecting at least one vote-switched precinct for recounting, of 0.9, 0.99, and 0.999 respectively. In each table, the number of precincts to be recounted is given for various values of p, the total number of precincts and for various values of d/2nx.

The tables show that, for constant p and x, as the candidate fractional difference d/n gets smaller, the number of precincts to be recounted becomes larger and approaches the total number of precincts. This accords with what one would intuitively expect, and what actually occurs in practice. When there are very small reported differences between candidates, there is a high likelihood of a recount being demanded.

4. Effect of Larger Number of Precincts

An interesting phenomenon, not intuitively obvious, can be seen from an inspection of the results. For equal values of d/2nx, the number of precincts to be recounted is roughly the same for significantly different quantities of total numbers of precincts. For example, if d/2nx = 0.1 and P = 0.9 (Table 1), then 22 precincts must be recounted, for total number of precincts equal to 500, 1000, 2000, or 5000. The percentage of precincts recounted is very different if 22 of 500 are recounted rather than 22 of 5000. The results show, therefore, that to minimize the absolute number of ballots recounted, there should be more precincts. More precincts are obtained by having fewer voters per precinct, but this may raise the cost of general administration.

5. More Complex Situations

At this point, only the simple situation of just two candidates, equal numbers of voters in each precinct, and no overvotes and undervotes, has been considered.

In an actual election, the number of voters per precinct is variable, not constant as has been assumed. The validity of the analysis presented depends upon the type of misreporting of precinct results with which the election administration expects to be confronted. If it could be assumed that vote-switched precincts occur randomly such that the mean size in voters per precinct of these precincts equals the average size of all precincts, i.e., n/p, then the expected number of misreported precincts will be the same as that computed by equation (3). On the other hand, it may be noted that if vote-switched precincts were larger than average size, fewer of them would be needed to overturn an election than the number computed by (3). One strategy that could be employed to guard against this possibility is for precincts to be selected for recounting with a probability proportional to the number of voters that each has. Other strategies could be adopted and there appears to be ample material for further investigations.

When there are undervotes and overvotes, as well as candidate votes, a vote switch can occur between a candidate and either an undervote or an overvote instead of between two candidates. If one candidate's votes are increased at the expense of overvotes or undervotes, an error could be introduced without disturbing a second candidate's votes at all. In this case the second candidate's fraction of total candidate votes remains larger than it would have if that candidate's votes were actually reduced by a vote-switch. Thus, there is less likelihood of detection by observation unless records have been kept on undervotes and overvotes, enabling unusual conditions to be discovered. However, undervotes and overvotes are nearly universally not reported at this time.

Similarly, with more than two viable candidates, the maximum level of undetectability by observation, as a practical matter, would be somewhat higher since the election would be more difficult to predict.

A vote switch could take small numbers of votes from several opposition candidates to benefit one candidate, thereby minimizing detection by observation.

One mitigating circumstance is that the calculations of equations (2) and (3) made to determine recount quantities were based on the minimum number of votes needed to switch an election outcome. The probability of a vote-switch with the minimum number of votes to overturn an election is small. Any smaller number of votes switched would have no effect on the outcome, and any larger number of votes switched (to further assure a specific outcome) would increase the probability of detection, either by partial recount or by observation.

6. Findings

An adequate partial recount quantity depends on the closeness of the vote, the total number of precincts involved, the value of the maximum level of undetectability by observation, and the desired probability of detection by recount. The latter two quantities can only be determined subjectively at this time.

In a close election, a flat 1% recount is insufficient to detect vote-switching of sufficient magnitude to overturn it.

Ballot reconciliations and reporting of overvotes and undervotes will reduce the opportunities for undetected vote switching.

Election administrators, candidates, and others interested in honest elections should keep well-documented records of voting patterns and expected numbers of overvotes and undervotes so that abnormal voting results can be more easily spotted and investigated. Such records may be used to develop a quantitative basis for such parameters as the "maximum level of undetectability by observation."

Dividing the electorate into a larger number of precincts will reduce the total number of ballots required to be recounted to maintain the same capability of detection of vote-switching.

Total Number of Precincts, p

d/2nx	50 Precincts	100 Precincts	200 Precincts	500 Precincts	1000 Precincts	2000 Precincts	5000 Precincts
0.005	50	100	181	301	369	411	439
0.01	50	91	137	184	205	217	224
0.02	46	69	87	102	108	111	113
0.05	30	37	41	43	44	45	45
0.1	18	20	21	22	22	22	22
0.2	10	10	11	11	11	11	11
0.5	4	4	4	4	4	4	4
1.0	1	1	1	1	1	1	1

Table 1. Number of Precincts to be Recounted, P=0.9

Total Number of Precincts, p

d/2nx	50 Precincts	100 Precincts	200 Precincts	500 Precincts	1000 Precincts	2000 Precincts	5000 Precincts
0.005	50	100	199	421	601	737	840
0.01	50	100	180	300	368	410	438
0.02	50	90	136	183	204	216	223
0.05	42	59	73	83	86	88	89
0.1	29	36	40	42	43	44	44
0.2	17	19	20	21	21	21	21
0.5	7	7	7	7	7	7	7
1.0	1	1	1	1	1	1	1

Table 2. Number of Precincts to be Recounted, P=0.99

Total Number of Precincts, p

d/2nx	50 Precincts	100 Precincts	200 Precincts	500 Precincts	1000 Precincts	2000 Precincts	5000 Precincts
0.005	50	100	200	468	748	996	1205
0.01	50	100	194	373	497	582	643
0.02	50	97	164	248	290	315	331
0.05	47	74	98	118	126	131	133
0.1	36	48	56	62	64	65	66
0.2	23	27	29	30	31	31	31
0.5	9	10	10	10	10	10	10
1.0	1	1	1	1	1	1	1

Table 3. Number of Precincts to be Recounted, P=0.999

Appendix C: REFERENCES

1. U.S. General Accounting Office Interagency Agreement with the National Bureau of Standards Institute for Computer Sciences and Technology, February 10, 1974, Procedures 1.

2. ibid. Procedures 1.C.

3. ibid. Purpose of Agreement.

4. Sidney B. Geller, "The Effects of Magnetic Fields on Magnetic Storage Media Used in Computers," U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., NBS Technical Note 735, July, 1972.

5. Susan K. Reed and Martha M. Gray, "Controlled Accessibility Bibliography," U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., NBS Technical Note 780, June, 1973.

6. Clark R. Renninger and Dennis K. Branstad, "Government Looks at Privacy and Security in Computer Systems," U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., NBS Technical Note 809, February, 1974.

7. Dennis K. Branstad and Susan K. Reed, "Executive Guide to Computer Security," U.S. Department of Commerce, National Bureau of Standards, Washington, D.C. and Association for Computing Machinery, New York, N.Y., NBS Special Publication.

8. Susan K. Reed and Dennis K. Branstad, "Controlled Accessibility Workshop Report," U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., NBS Technical Note 827, May, 1974.

9. Clark R. Renninger, "Approaches to Privacy and Security in Computer Systems," U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., NBS Special Publication 404, September, 1974.

10. Data on commencement of punch card voting supplied by Computer Election Systems, Inc., 1001 Eastshore Highway, Berkeley, California 94710.

11. Council of State Governments, Modernizing Election Systems, Lexington, Kentucky, 1973, p. 31.

12. San Francisco Chronicle, "The San Francisco Vote Count--Another Disaster," November 6, 1968, p. 1:3.

13. Computerworld, "Election Errors Are Laid to People," December 11, 1968, p. 1:1.

14. San Francisco Chronicle, "Vote Tally by Computer Assailed," November 18, 1968, p. 6:1.

15. San Francisco Chronicle, "12,000 Mysterious San Francisco Votes," November 22, 1968, p. 1:6.

16. San Francisco Chronicle, "Those Votes That Weren't Counted," November 25, 1968, p. 46:1.

17. Computerworld, "'Modest' Devices Hasten Reporting of Election Returns," by William T. Ziegler, October 30, 1974, p. S/5.

18. Economics Research Associates, "Determination of the Causes of June 2, 1970 Primary Election Problems and Recommendations for Correction," July 2, 1970, Los Angeles, California.

19. Computerworld, "California Controversy Over Vote Count Threatens Use of Punched-Card Method," by Phillis Huggins, June 10, 1970, p. 1.

20. American University Institute of Election Administration and National Scientific Corporation, "A Study of Election Difficulties in Representative American Jurisdictions, Final Report," January, 1973, for Office of Federal Elections, Washington, D.C., p. VI 28-31.

21. Computerworld, "The California Elections: A DP Manager's Nightmare," by Phyllis Huggins, June 17, 1970, p. 2:1.

22. Anonymous, "Who Put the Late in Vote Tabulate?," Datamation, July 15, 1970, p. 123.

23. Computerworld, "L.A. Braces for November 3 Vote, Adds Innovations, Security," by Phyllis Huggins, October 28, 1970, p. 1:1.

24. Computerworld, "L.A. Vote Count Succeeds, Loose Chads Still Problem," by Phyllis Huggins, November 11, 1970, p. 4:1.

25. Fresno Bee, "'Bugs' Bug County Vote-Tally Plan," June 1, 1970, p. 1.

26. Fresno Bee, "Fresno Computer Lag Will Delay Vote Count," June 2, 1970, p. 1:1.

27. Fresno Bee, "Fresno Vote Fiasco Spurs Calls for Probe," June 3, 1970, p. 1:1.

28. Fresno Bee, "People Errors Delayed Tallies in 3 Counties," June 4, 1970, p. 1:1.

29. Fresno Bee, "Craven: 'So What?' About Vote Foul Up," June 7, 1970, p. 2C.

30. Aubrey Dahl, "Burning Issue at Stake in General Election. So Who Counts?," Datamation, November 1, 1970, p. 48, 49.

31. National Scientific Corporation, "Violations of the Election Laws and Procedures, Special Detroit Primary Election, August 4, 1970," 7115 Leesburg Pike, Falls Church, Virginia 22043, August 25, 1970.

32. American University Institute of Election Administration and National Scientific Corporation, op. cit. p. VI-37.

33. Metropolitan Detroit Chapter, Association for Computing Machinery, "Technical Analysis of the City of Detroit Punched-Card Voting Experiences of 1970," mimeographed May 14, 1971, p. 23.

34. National Scientific Corporation, op. cit., p. III-1.

35. Enclosures submitted by George C. Edwards, City Clerk of Detroit and Chairman, City Election Commission to Honorable Mel Ravitz, President of the Common Council and Honorable Henry L. Heading, Judge of Recorder's Court, August 28, 1970: Minutes of Meeting, August 6, 1970, p. 5.

36. National Scientific Corporation, op. cit., p. II-6.

37. Enclosures submitted by George C. Edwards, op. cit.: Minutes of Meeting, August 6, 1970, p. 4.

38. National Scientific Corporation, op. cit., p. II-7.

39. Enclosures submitted by George C. Edwards, op. cit.: Minutes of Meeting, August 6, 1970, p. 2.

40. Enclosures submitted by George C. Edwards, op. cit., Report on Punch Card Voting System to City of Detroit, by J. E. Hall, Datamedia Services, Inc., p. 4.

41. Enclosures submitted by George C. Edwards, op. cit., Minutes of Meeting, August 6, 1970, p. 4.

42. ibid.

43. Enclosures submitted by George C. Edwards, op. cit., Memo to Mel Ravitz and Judge Henry L. Heading, August 27, 1970, p. 3.

44. Metropolitan Detroit Chapter, Association for Computing Machinery, op. cit., p. 26.

45. Enclosures submitted by George C. Edwards, op. cit., Memo to Mel Ravitz and Judge Henry L. Heading, August 27, 1970, p. 4.

46. Metropolitan Detroit Chapter, Association for Computing Machinery, op. cit., p. 25.

47. Enclosures submitted by George C. Edwards, op. cit., Memo to Mel Ravitz and Judge Henry L. Heading, August 27, 1970, p. 3.

48. Wall Street Journal, "And the Winner Is...? Computer Is the Loser in Michigan Election," by Art Glickman, August 6, 1970, p. 1.

49. Computerworld, "Detroit is Singing the Computerized Vote Count Blues," by Edward J. Bride, August 12, 1970, p. 4:1.

50. Detroit News, "Punch Card Voting Is Success Again in Detroit," by Mike Maza, November 8, 1973, p. 17-B.

51. Computerworld, "Tested Vote System Felled by Programmer's Error," September 6, 1972, p. 1.

52. Letter in the files of the Michigan State Election Division, Lansing, Michigan from Ray Clements of Houston, Texas to George Herstek of the State Election Division, received August 15, 1972.

53. Houston Post, "Big Vote Causes Confusion," November 8, 1972, p. 1:4.

54. Houston Post, "Federal Probe of Punch Card Ballots Sought," November 10, 1972, p. 4A:7.

55. Houston Post, "GOP Wants Recount," November 12, 1972, p. 1:6.

56. Washington Post, "Recount Seems to Back Computer Totals," by Linda Newton Jones, September 22, 1974, p. C1.

57. Washington Star-News, "Alexander Concedes to Mayor," September 11, 1974, p. A1, B5.

58. Washington Post, "Vote Count a $120,000 D.C. Fiasco," September 12, 1974, p. B4.

59. ibid.

60. Washington Star-News, "No Change in Winners as D.C. Recount Ends," by Lance Gay, September 23, 1974, p. B1.

61. Washington Post, "Computer Firm Blamed in Vote Tally," by Linda Newton Jones, September 27, 1974, p. D1, D2.

62. Internal CDC memos supplied to a representative of NBS at a meeting with Control Data Corporation management representatives on November 8, 1974, at CDC local headquarters, Rockville, Md.

63. Washington Post, "The City's Bungling of the Ballots," August 29, 1974, p. A30:1.

64. Memo to Eugene L. Bennett, Material Management Officer from Norval E. Perkins, Executive Secretary, Board of Elections and Ethics, October 15, 1974, p. 2.

65. Washington Star-News, "Tale is Told of District's 'Missing' Votes," by Michael Kiernan, September 25, 1974, p. B1.

66. Letter, dated November 16, 1970, in the files of the Department of Finance, City of Flint, Michigan, from W. R. Penberthy, Data Processing Administrator to Robert M. Patterson, Executive Editor, Computerworld.

67. Computerworld, "A Rainy Day in Flint," November 11, 1970, p. 4.

68. Letter dated June 24, 1974 in the files of the National Bureau of Standards from Val Guerrier, Deputy City Clerk, City of Flint to Roy G. Saltman, NBS.

69. Computerworld, "D.C. Primary Snarl Blamed on In-House Printed Cards," January 20, 1971, p. 2.

70. Donn B. Parker, Susan Nycum, and S. Stephen Oüra, Computer Abuse, Stanford Research Institute, November 1973, p. 110.

71. Los Angeles Free Press, "Baxter Ward Charges Vote Irregularity by Computer," by Ridgely Cummings, April 27, 1973, p. 1.

72. Computerworld, "Accuracy of L.A. Vote System Challenged," by Marvin Smalheiser, May 5, 1973, p. 5.

73. Memo dated November 10, 1972, from Mr. Ronald Del Monte, Data Processing Manager, Travis County, in the files of the County Clerk, Travis County, Austin, Texas.

74. Memo dated November 9, 1972, from Mr. Robert Carey in the files of the County Clerk, Travis County, Austin, Texas.

75. Seattle Post-Intelligencer, "For Want of a Card: Chaos," September 21, 1973, p. 1:4.

76. Computerworld, "Two Input Errors Plague Seattle Election," October 10, 1973, p. 4:2.

77. Seattle Post-Intelligencer, "Election Night Crisis." September 27, 1973, p. A10.

78. The variation in the card lengths was demonstrated to National Bureau of Standards representatives.

79. Computerworld, "Delays, Errors Put Damper On Some Election Counts," by Edie Holmes, June 19, 1974, p. 1:4.

80. Situation verified verbally by the office of the Elections Coordinator, State of Oregon.

81. Los Angeles Times, "Experts Game: How Elections Can Be Rigged by Computer," by Richard Bergholz, July 8, 1969, p. 1:1.

82. New York Times, "Los Angeles to See If Cheats Can Rig an Elections Computer," July 13, 1969, p. 64:6.

83. Washington Post, "Cheating on Vote Tally Eyed," July 24, 1969, p. F6.

84. Jack Harrison Pollack, "Six Ways Your Vote Can Be Stolen," Harper's, November, 1972, p. 88, 89.

85. Los Angeles County Board of Supervisors, Report of the Los Angeles County Elections Security Committee, 713 Hall of Administration, Los Angeles, California 90012, March 3, 1970.

86. James Farmer, Colby Springer, and Michael Strumwasser, "Cheating the Vote-Count Systems," Datamation, May, 1970, p. 76-80.

87. ibid., p. 79.

88. Robert L. Patrick and Aubrey Dahl, "Voting Systems," Datamation, May, 1970, p. 81, 82.

89. Economics Research Associates, "Phase II Implementations and Recommendations for Election Security," July 31, 1970, Los Angeles, California.

90. Isaacs Associates, Inc., Final Report, County of Los Angeles Votomatic Computer System Audit - Volume I - "Summary of Major Findings and Recommendations," 1100 Glendon Avenue, Los Angeles, California 90024, December 1, 1970.

91. Isaacs Associates, Inc., op. cit., Volume II - "Technical Conclusions and Recommendations."

92. Walter V. Sterling, Inc., Final Report. Study of Punchcard Voting System Security, Prepared for California State Commission on Voting Machines and Vote Tabulating Devices, Claremont and Los Altos, California, June 1970.

93. Memorandum from Adrian Kuyper, County Counsel (Orange County, California) to Members of the Board of Supervisors, August 3, 1973, on the subject "Opinion of the Legislative Counsel: FMO Contract."

94. Anonymous, "We owe an apology," Computer Decisions, July 1974, p. 69:3.

95. Stuart Baur, "The Long Playing, Widespread, Supermarket Checkout Rip-Off," New York, vol. 7, no. 35, September 2, 1974, p. 25.

96. American Federation of Information Processing Societies, Inc., Systems Review Manual on Security, 1974, Montvale, New Jersey 07645.

97. National Bureau of Standards, Guidelines for Automatic Data Processing Physical Security and Risk Management, Federal Information Processing Standard Publication (FIPS PUB) 31, June 1974, U.S. Government Printing Office, Washington, D.C. 20402.

98. National Bureau of Standards, op. cit., p. 56.

99. ibid., p. 56.

100. ibid., p. 60.

101. Eric J. Novotny, "Democracy by Computer: Design, Operation, and Implementation of a Civic Communications System," in The Systems Approach: Key to Successful Computer Applications, Thirteenth Annual Technical Symposium Sponsored by Washington, D.C. Chapter, Association for Computing Machinery and Institute for Computer Sciences and Technology, National Bureau of Standards, June 20, 1974.

102. W. W. Peterson and D. T. Brown, "Cyclic Codes for Error Detection," Proc. I.R.E., vol. 49, no. 1, January 1961, pp. 228-235.

103. Paul Kreager, "Small Computer Cyclic Redundancy Checksum Capability," Computer Design, May 1972, pp. 95-98.

104. ANSI X3534/484, "Performance of the SDLC, CRC-16, and CCITT Polynomials with NRZI Coding," submitted by Donald C. Johnson, April 3, 1972; memo available at the Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234.

105. Norris S. Goff, "Development Project Costs," Journal of Systems Management, September 1974, p. 14.

106. Adapted from Joseph J. Moder and Cecil R. Phillips, Project Management with CPM and PERT, New York, New York, Reinhold Publishing Corp., 1964; Figure 11-5, p. 271.

107. State of Arizona, Electronic Voting System Instructions and Procedure Manual, compiled by Wesley Bolin, Secretary of State, Revised August 20, 1974, pp. 2-61.

108. American University Institute of Elections Administration and National Scientific Corporation, op. cit., p. VIII-8.

109. ibid., p. VIII-12.

110. ibid., p. VII-18.

111. Ivan Flores, "Computer Software," Science and Technology, May 1969, p. 16.

112. X3.23 - 1974 Programming Language COBOL, American National Standards Institute, 1430 Broadway, New York, N.Y. 10018

113. X3.9 - 1966 FORTRAN (DOD), American National Standards Institute, New York, N.Y.

114. X3.10 - 1966 Basic FORTRAN (DOD), American National Standards Institute, New York, N.Y.

115. National Bureau of Standards, Common Business Oriented Language COBOL, (FIPS PUB 21), March 15, 1972, U.S. Government Printing Office, Washington, D.C. 20402.

116. Russell M. Armstrong, Modular Programming in COBOL, John Wiley & Sons, New York, 1973, pp. 59-71.

117. State of California Commission on Voting Machines and Vote Tabulating Devices, Reliability Demonstration Test Specification for Electronic and Mechnical Vote Recording and Tabulating Equipment, issued November 5, 1968.

118. Computerworld, "Delays, Errors Put Damper on Some Election Counts," by Edie Holmes, June 19, 1974, p.2:2.

119. Computerworld, "Officials Stress Public Education", by Edith Holmes, October 16, 1974, p.1:1.

120. Council of State Governments, Power to the States - Mobilizing Public Technology, (Report and Supporting Analyses) May 1972, Lexington, Kentucky 40505, p. xiv.

121. ibid., p. xiv, xv.

122. National Municipal League, A Model Election System, 1973, New York, New York, p. 12.

123. Comments by Mrs. Marie Garber, Elections Administrator, Montgomery County, Maryland enclosed with letter to Mr. Richard J. Carlson, Director, Elections Systems Project, National Municipal League, May 21, 1973, p. 1.

124. League of Women Voters Education Fund, Administrative Obstacles to Voting, 1972, Washington, D.C., p. 23.

125. ibid., p. 23.

126. National Municipal League, op. cit., p. 12.

127. ibid., p. 13.

128. Comments by Mrs. Marie Garber, op. cit., p. 1.

129. National Municipal League, op. cit., p. 16.

130. Comments by Mrs. Marie Garber, op. cit., p. 2.

131. National Municipal League, op. cit., p. 10.

132. ibid., p. 7.

133. State of Arizona, op. cit., p. 64-72A.

134. State of Michigan, Elections Division, Interim Rules for Electronic Voting Systems 1974, p. 1-5.

135. League of Women Voters Education Fund, op. cit., p. 22.

136. ibid., p. 19.

137. National Municipal League, op. cit., p. 16.

138. Anonymous, "But What If You Get A Wrong Number?", Datamation, March, 1974, p. 17.

139. Letter, dated October 3, 1974, in the files of the National Bureau of Standards, from John J. Pearson, Assistant Supervisor of Elections, State of Washington, to Roy G. Saltman, NBS.

140. Washington Star-News, "Voiceprint Evidence Barred", by David Pike, June 7, 1974, p. B-2.

141. Washington Post, "Appeals Court Bars Voiceprint Evidence", by Eugene L. Meyer, June 7, 1974, p. 1, 14.

142. ibid.

143. Council of State Governments, Power to the States - Mobilizing Public Technology, (report and supporting analyses) May 1972, Lexington, Kentucky 40505, p. 178.

144. Council of State Governments, Modernizing Election Systems, December, 1973, Lexington, Kentucky 40511, p. 8.

145. ibid., p. 9.

146. ibid.

147. Kranzley & Co. Applied Telecommunications Division, "Synchronous Data Link Control, Part 1 - General Concepts & Structure", Modern Data, February, 1975, p. 25, 26.