PERFORMANCE AND TEST STANDARDS

FOR

PUNCHCARD, MARKSENSE, AND DIRECT RECORDING ELECTRONIC VOTING SYSTEMS

FEDERAL ELECTION COMMISSION

January, 1990

For sale by the Superintendent of Documents, U.S. Government Printing Office Washington, D.C. 20402

APRIL 1990 REVISIONS TO THE PERFORMANCE AND TEST STANDARDS

Abstract

Revised page xxiii to reflect corrections made in Section 4 regarding high level language and structured programming.

Section 4

Revised Subsection 4.2 to correct contradictory language regarding use of high level language and structured programming, and to repeat restrictions on module entry and exit noted in Appendix E.

Section 5

The last sentence of Subsection 5.3 was revised to clarify that the security penetration analysis shall not be routinely distributed to jurisdictions that program elections. The analysis shall, however, be included in the material the vendor deposits in escrow.

Section 7

The last paragraph of Subsection 7.4.2 has been changed to state that egregious instances of non-compliance to acceptable software design procedures will be cause for failure.

Appendix B

Subsection B.3.3.5.4 has been revised to make it clear that this section refers to operating procedures for maintaining the security of the software.

In Subsection B.3.5, the Security Analysis description has been revised to clarify that the security penetration analysis shall not be routinely released to jurisdictions responsible for programming elections.

Appendix E

Clarified Subsection E.2 regarding the use of unconditional branching, such as GOTOs, in computer programs.

ACKNOWLEDGMENTS

The *Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems* were developed by Robert Naegele, under contract to the Federal Election Commission. Penelope Bonsall, Director of the FEC's National Clearinghouse on Election Administration, served as the technical contract manager for the project. The accompanying documents, *A Plan for Implementing the FEC Voting Systems Standards*, the *System Escrow Plan*, and *A Process for Evaluating Independent Test Authorities*, were drafted and written in large part by the Clearinghouse staff.

These products were, in actuality, the combined efforts of many. A multitude of practical insights have been provided by the Clearinghouse's Advisory Panel:

The Honorable Richard Austin
Secretary of State
Michigan

The Honorable Allen J. Beermann
Secretary of State
Nebraska

The Honorable Roy Blunt
Secretary of State
Missouri

The Honorable Sherrod Brown
Secretary of State
Ohio

The Honorable Jane Carroll
Supervisor of Elections
Broward County
Florida

The Honorable Marge Christianson
Supervisor of Elections
Hennepin County
Minnesota

The Honorable Max Cleland
Secretary of State
Georgia

The Honorable Bremer Ehrler
Secretary of State
Kentucky

The Honorable Emmett H. Fremaux, Jr.
Executive Director
Board of Elections and Ethics
Washington, DC

The Honorable Douglas Jernigan
Supervisor of Elections
Montgomery County
Maryland

The Honorable Stanley Kusper, Jr.
Cook County Clerk
Illinois

The Honorable Natalie Meyer
Secretary of State
Colorado

The Honorable Ronald D. Michaelson
Executive Director
State Board of Elections
Illinois

The Honorable Ralph Munro
Secretary of State
Washington

The Honorable Barbara Rossetti
Assistant Secretary
Tulsa Board of Elections
Oklahoma

The Honorable Anita Rodeheaver
County Clerk
Harris County Courthouse
Texas

The Honorable Deborah Seiler
Chief Consultant
Assembly Elections Committe
California

The Honorable Jim Shumway
Secretary of State
Arizona

The Honorable Thomas W. Wallace
Executive Director
State Board of Elections
New York

The Honorable Charles Weissburd
Registrar-Recorder
Los Angeles County
California

Appreciation must be given to numerous other state and local election officials who assisted in this review process. Some who deserve special thanks are: Shirley Baccus, Marie Brewer, Laurie Christie, P. Michael Cinnamon, Hoyt Clifton, Stuart Cohen, Joseph DiStefano, Kathleen Doran, Enid Earle, Susan Farmer, Jerry Fowler, Marie Garber, J. Phil Gilbert, Robert Grant, Ernest Hawkins, Jean-Marc Hamel, William Huish, Clara Jones, Charles Kaniss, Michael Lavelle, Ed Mahoney, James Malone, Daniel Nelson, Ray Phelps, Sam Reed, Lyall Schwarzkopf, Sandy Steinbach, Don Siegelman, Don Whiting and Thomas Wilkey.

Over several years, a distinguished group of technical experts gave generously of their time and provided this project with valuable assistance.

William Detlof
Elections Systems, L.A. County
Data Processing Department
Downey, CA

Ralph Heikkila
Assistant Registrar-Recorder
Technical Services
Los Angeles, CA

Dr. Lance Hoffman
School of Engineering
George Washington Univ.
Washington, DC

Ron Kopp
Information Technology Group
Ernst & Young
Los Angeles, CA

Roy Saltman
National Institute of Standards and Technology
Gaithersburg, MD

Malin Van Antwerp
ECRI
Plymouth Meeting, PA

Dr. Willis Ware
The Rand Corporation
Santa Monica, CA

Douglas Webb
SRI International
Menlo Park, CA

Dr. Britain J. Williams
Office of Computing Services
GTRI
Atlanta, GA

Last, but certainly not least, Congressional staff, public interest groups, and representatives from vendors of punchcard, marksense, and direct recording electronic systems were most helpful in providing comments, highlighting discrepancies, and, ultimately, creating a more useful final product.

TABLE OF CONTENTS

Page

Page

Page

Page

Page

Page

Page

Page

ABSTRACT

State and local officials today are confronted with voting system failures and increasingly complex voting system technology. The U.S. Congress, responding to calls for assistance from the states, authorized the Federal Election Commission (FEC) to develop national voting systems standards for computer-based systems, but mandated that they be voluntary. The resulting FEC Voting System Standards Project seeks to aid state and local election officials in ensuring that new voting systems are designed to function accurately and reliably. States are free to adopt the standards in whole or in part, or reject them. States may also choose to enact stricter performance requirements for systems to be used in their jurisdictions.

A series of public hearings were held as the standards were being developed. State and local election officials, representatives of election system vendors, pro bono technical consultants, and others reviewed drafts of the proposed criteria. The FEC considered their many comments and, where appropriate, made corresponding revisions. Before final issuance, the FEC publicly announced the availability of the latest draft of the standards in the *Federal Register* and requested that all interested parties submit their final comments. The FEC meticulously reviewed all responses to the notice and incorporated corrections and suitable suggestions. The final product, therefore, is the result of considerable deliberation, close consultation with election officials, and careful consideration of comments from other interested persons.

In January 1990, the FEC approved for issuance the performance standards and testing procedures for punchcard, marksense, and direct recording electronic voting systems. The standards do not cover paper ballot and mechanical lever systems. The FEC also did not incorporate requirements for mainframe computer hardware within the hardware standards, since it was reasonable to assume that other engineering and performance criteria govern the operation of mainframe computers. Vote tally software installed on mainframes, however, is covered by the standards.

The standards specify general performance criteria, as well as detailed test criteria. Essentially, they address what a voting system should reliably do, not how the system should meet this requirement. It is not the intent of the standards to impede the design and development of new, innovative equipment by vendors. Furthermore, the standards ought not force vendors to price their voting systems out of the range of local jurisdictions.

The FEC also produced three companion documents that discuss aspects of implementing the standards. One, entitled *A Plan for Implementing the FEC Voting System Standards*, presents recommended strategies and issues that states may consider during standards implementation. A second, the *System Escrow Plan for the Voting System Standards Program*, explains the proposed escrow of proprietary voting system software and documentation. The third, *A Process for Evaluating Independent Test Authorities*, describes the proposed process for evaluating the national test authorities that will examine the voting systems for their compliance with the standards. In the future, the FEC will complete associated procedural guidelines covering voting system procurement, computer security, pre-election day testing, and system operations.

Background

Much of the groundwork for the standards development was laid by a national study conducted by the National Bureau of Standards, now known as the National Institute of Standards and Technology. This study had been requested by the FEC's predecessor, the Office of Federal Elections of the General Accounting Office. Entitled *Effective Use of Computing Technology in Vote-Tallying*, the 1975 report made a number of recommendations bearing directly on the standards project. After analyzing computer-related election problems encountered, the report concluded that one of the basic causes for these difficulties was the lack of appropriate technical skills at the state and local level for developing or implementing sophisticated and complex written standards, against which voting system hardware and software could be tested.

Following the release of this report, the U.S. Congress mandated that the FEC, with the cooperation and assistance of the National Bureau of Standards, study and report on the feasibility of developing "voluntary engineering and procedural performance standards for voting systems used in the United States." (See P.L. 96-187.) The resulting 1983 study cited a substantial number of technical and management problems which affected the integrity of the vote counting process. It also detailed the need and desirability of having a federal agency develop national performance standards that might be used as a tool by state and local election officials in their testing, certification, and procurement of computer-based voting systems. In 1984, Congress approved initial funding for the standards project.

Relevance

A primary goal of the standards, and related test procedures, is to assist state and local officials in assuring the public of the automated election system's integrity. This may be accomplished by establishing industry-wide minimum criteria for punchcard and marksense (P&M) and direct recording electronic (DRE) voting systems, and

future systems that function comparably. Consequently, the standards include minimum:

- functional requirements;
- performance characteristics;
- documentation requirements; and
- test evaluation criteria.

The functional requirements and hardware, software, security, quality assurance, and documentation standards described in Sections 1-6 are relevant to:

- state or local agencies evaluating voting systems to be procured within their jurisdiction;
- designers and manufacturers of voting systems; and
- authorities responsible for the analysis and testing of such systems.

Qualification testing specifications and documentation requirements, detailed in Section 7 and Appendices B, and F through I, are of primary importance to independent test authorities responsible for the analysis of voting systems during qualification testing, described below. However, these sections are also relevant to voting system developers, manufacturers, and states which must certify a system prior to procurement by a local jurisdiction. Vendors and jurisdictions involved in acceptance testing will reference Section 8 and Appendices B, G, and J.

Systems that are tested and meet the basic requirements specified in Sections 1 through 8 and related Appendices B, C, F, G, H, I, and K will have been shown to be reliable, accurate, and capable of secure operation before being used in elections. Systems that also conform to the recommended design guidelines in Appendices A, D, and E, and that pass optional tests (e.g.; sand and dust exposure, rain exposure) will provide additional assurance of successful operation and ease of maintenance.

Application of the Standards and Test Specifications

In general, the standards define performance characteristics that can be assessed by a series of quantitative tests and qualitative examination. The standards apply to system hardware and software developed by a vendor, and software developed in-house by state or local jurisdictions, including software designed for use with off the shelf hardware.

The standards call for the examination of equipment and ballot tally software used in computer-based vote tally systems to determine their suitability for election use. All products composing the voting system shall be tested during functional system-level testing. In addition, most hardware and software designed or modified for election use shall submit to other rigorous tests and selectively in-depth source code review. Those products that are excepted from all but the functional tests are noted in Section 7.1.1.2.

System hardware and software, other than grandfathered products, shall be subject to the following three testing phases prior to being purchased or leased:[1]

- **Qualification tests** shall be performed by an independent test authority. Qualification tests encompass the selectively in-depth examination of software; the inspection and evaluation of system documentation; tests of hardware under conditions simulating the intended storage, operation, transportation, and maintenance environments; and operational tests verifying system performance and function under normal and abnormal conditions. The scope of qualification testing should not be confused with the vendor's developmental testing. Qualification testing is the process by which a voting system is shown to comply with the requirements of its own design specification and with the requirements of the standards. The ITA will be expected to evaluate the completeness of the vendor's developmental test program, including the sufficiency of vendor tests conducted to demonstrate compliance with performance specifications. The ITA will undertake sample testing of the vendor's test modules and also design independent system-level tests to supplement and check those designed by the vendor.

- **Certification tests** shall be performed by individual states, with or without the assistance of outside consultants. Certification test criteria are not included in the standards, as they must be defined by the state, with state laws, election practices, and specific environment in mind. It is recommended, however, that they not duplicate qualification tests, but include functional tests and qualitative assessment to ensure that the system operates in a manner that is acceptable under state law.

- **Acceptance tests** shall be performed at the local jurisdiction level to evaluate the degree to which delivered units conform to both the system characteristics specified in the procurement documentation, and those demonstrated in the qualification and certification tests. Some of the

1/ For further information on the application of the standards and testing criteria to grandfathered systems, refer to the FEC document entitled, *A Plan for Implementing the FEC Voting System Standards* (hereafter referred to as the "implementation plan").

operational tests conducted during qualification would be repeated during acceptance testing.

Further examination of a system would be required after the system has completed qualification testing if modifications are made to hardware or software, or the software package is installed in different hardware. The independent test authority will determine if the system should be resubmitted for qualification testing. In the case of software modifications, as distinct from hardware changes, requalification testing is likely. The modified system might also need to be reexamined by the states and user jurisdictions to determine if further certification and acceptance testing is warranted.[2]

It is recommended that local jurisdictions perform pre-election logic and accuracy tests on all systems prior to their use in an election. These tests ensure that the system software has been coded correctly for the upcoming election, that required data has been entered correctly, and that system components such as ballots and programmable memory devices have been properly prepared. Pre-election tests are not covered in detail in the standards. They will, instead, be discussed in the companion voting system management guidelines that are to be produced by the FEC in the future.

Functional Specifications

Critical functions relevant to the successful performance of punchcard, marksense, and direct recording electronic systems are described in Section 2 of the standards. These functions include all of the operations necessary to prepare the system for an election, to conduct an election, and afterwards to obtain the vote count and audit report, and preserve the system for future use (i.e.; ballot definition, programming and software installation, equipment and system readiness tests, opening the polling place, voting selections and options, closing the polling place, and obtaining reports).[3] Provisions for overall system security, accuracy and integrity, and data retention are also discussed.

Hardware Requirements

Hardware performance requirements for punchcard, marksense, and direct electronic voting systems are specified in Section 3. Requirements for documenting the hardware configuration and development process are also included. The performance characteristics include requirements for:

2/ Further discussion of this process is included in the implementation plan.

3/ These functional categories are mirrored in the failure definitions of Appendix G.

- shelter, space, furnishings and fixtures, energy supply, temperature ranges, and telecommunications capabilities;
- hardware (and related software) needed to prepare and validate ballots for each voting device;
- devices (and related software) and procedures necessary to prepare, test, enable and disable voting devices, to detect and recover from errors; and, if required, to produce a consolidated report of data from all voting devices at the polling place;
- vote recording equipment and materials (e.g.; ballots, punching or marking devices, voting booths, public and protective counters, and electronic vote recording speed, accuracy, and reliability);
- ballot reading and handling devices in punchcard and marksense systems;
- memory and cartridge device stability for retention of control programs and data;
- equipment necessary to print vote totals and to transmit voting data to remote locations; and
- equipment required to process and report voting data after it has been consolidated at the polling place, including the processing of absentee and exception ballots.

In addition, this section defines physical characteristics, such as categories of equipment by weight, and general requirements for transport and storage, security, and transportability. General design, construction and maintenance characteristics are specified for durability, reliability, maintainability, availability, and transportability. General requirements are noted for materials and parts, ballot cards, ballot printing, punching styluses, vote recorders, electromagnetic radiation, product marking, workmanship, interchangeability, safety, and the capability to withstand environmental conditions present during operation, transportation, and storage. The hardware standards also specify human engineering requirements and reference related design guidelines in Appendix D.

Software Requirements

Specific software characteristics critical to the successful operation and maintenance of the voting system are delineated in Section 4. A number of these software standards impact on hardware, due to the interdependence of software and hardware in performing certain functions.

The software standards state required design and coding practices, including the use of modular programming techniques. Modular programming is a process by which the task is divided into programmable units or modules, each of which perform a single function. Each module can be tested and verified more or less independently of the remainder of the program. Modular programs place restrictions on module entry and exit conditions, and combat what has come to be known in the computer industry as "spaghetti code".

The design and coding requirements allow vendors to write software programs in either high level or assembly languages, or a combination of both. The use of a high level language (e.g.; Ada, COBOL, C, or Pascal) in voting system software is preferable for segments of the program associated with logical and numerical operations on vote data, but it is not required. High level language supports structured programming, which minimizes the likelihood of structural or or logic programming errors.

The standards also delineate software documentation requirements. Required data quality assessment characteristics are described. Standards for ballot interpretation logic, accuracy and integrity, data preservation, and audit trails are also presented.

The standards require DRE systems to incorporate multiple memories, both in the voting machine itself and in programmable memory device(s), where there is no paper ballot that can serve as a redundant means of verifying or auditing election results. DRE systems must also maintain, via an independent processing path, an electronic image of the ballot cast by each voter. These requirements better ensure the integrity of the process and provide data for recounts in contested elections.

All voting systems must provide an audit trail of system activity related to the vote tally. The primary objective of this requirement is the maintenance of a concrete, indestructible archival record of all system activity by which the correctness of the reported results may be verified. Such a record is essential for public confidence, for recounts, and in the event of litigation. The system design must prevent the program control or any individual from interfering with or terminating the audit trail. The system must also incorporate a real-time clock to provide the time and date of each audit record entry.

Four types of audit records are distinguished in Section 4. These records track:

- election definition and ballot formatting prior to election day (e.g.; log of baseline ballot formats and modifications thereto);

- the actions of the individuals and machines during election processing (e.g.; log of system status, error, and exception messages, records of any operator intervention, etc.);

- tests of system readiness prior to the casting and counting of ballots (e.g.; records of hardware and software diagnostic test results, the identification of the election to be processed, the identification of the software release); and

- the vote tally (e.g.; records of the number of ballots processed and vote totals including blank ballots and overvotes).

Records from election definition and ballot preparation work may include manual data; the remaining audit records must be automatically created and maintained by the system. Error messages must be reported unambiguously as they occur in order that immediate corrective action may be taken. Status messages must also be displayed unambiguously, but, depending on the critical nature of the message and the needs of the election jurisdiction, may or may not be displayed at the time of occurrence.

Security

Section 5 specifies additional security requirements tied to the technical aspects of hardware, software, and communications security. The vendor is obligated to incorporate access controls, and physical and telecommunications security measures. Certain precautions relating to software and firmware installation must also be observed.

Not all security requirements are enumerated within the standard. Pertinent administrative and management controls, internal procedures, physical facilities, organizational responsibilities, and pre-election day testing procedures will be specified in the companion voting system management guidelines that will be established by the FEC. Other technical aspects will be defined by the vendor, because of system-specific characteristics and operations.

The standards require developers and manufacturers of voting systems to incorporate security measures in the systems which they produce. Independent test authorities will then be responsible for analyzing each system's security provisions, and for devising tests to try to compromise the system.

Quality Assurance

Section 6 obligates the manufacturer of the voting system to install and operate a quality control program. This program will ensure that the design, workmanship, and

performance requirements of the standards are met by all delivered systems and components. The quality assurance program provides for the proper testing, operation, and maintenance of the systems and components, and requires vendors to maintain hardware and software developmental and test data. Complete product documentation is required under this section, and is defined in Appendix B. The documentation requirements include items such as the Vote Manual, System Operations Manual, System Maintenance Manual, a Hardware Specification, and a Software Specification.

Qualification Test and Measurement Procedures

Section 7 provides specifications for hardware, software, and system-level qualification tests. Compliance with the requirements of the performance standards will be assessed by means of these tests, conducted by an independent test authority.

Hardware qualification testing includes non-operating tests that require the use of an environmental test facility, and operating tests that are performed partly in an environmental facility and partly in a nominal test laboratory or shop environment. Non-operating tests are intended to evaluate the ability of the system to withstand various environmental conditions incidental to voting system storage, maintenance, and transportation. They include transit drop, bench handling, vibration, low and high temperature, humidity, and optional rain exposure, and sand and dust exposure tests. Operating tests involve utilizing the hardware for an extended period of time under varying temperatures and voltages to assess the hardware's reliability and its data reading and processing accuracy in potential election environments.

The hardware test requirements apply in full to all equipment used in a voting system with the exception of the following:

- commercially available models of general purpose data processing equipment that were designed to ANSI or IEEE standards, that have a broad field history of meeting the relevant requirements of the standards, and that have demonstrated compatibility with the voting system, or that otherwise have demonstrated compliance with these requirements (e.g.; Documation and PDI card readers);

- production models of special purpose data processing equipment that have a history of performing successfully under conditions equivalent to the election use, and that have demonstrated compatibility with the voting system (e.g.; Chatsworth card readers); and

- any ancillary devices that do not perform ballot reading, data processing, or the production of an official output report, and that do not interact with these system functions (e.g.; modems used to broadcast results to the press,

printers used to generate unofficial reports, or CRTs used to monitor the vote counting process).

Such equipment will be subject to functional and operating tests performed during software evaluation and system-level testing; however, they need not undergo hardware non-operating tests. If the system is composed entirely of off the shelf hardware, then such equipment also need not be subject to the 48-hour environmental chamber segment of the hardware operating tests.

Software qualification encompasses an evaluation of the sufficiency of software documentation, a selectively in-depth examination of source code, an appraisal of the software's structure and content, and the performance of functional tests.

Software qualification is applicable to the following:

- application programs that control and carry out ballot processing;
- specialized compilers and specialized operating systems associated with ballot processing; and
- ANSI standard language compilers and operating systems that have been modified for use in the vote counting process.

Normally, only ballot processing (as distinct from ballot layout) software shall be subjected to code inspection. For DRE systems incorporating independent processing paths, each path or module shall be evaluated. The examination of source code will include an evaluation of its logical correctness, the implementation of algorithms, and the software's modularity and construction. This review will also assess such attributes as simplicity, understandability, testability, robustness, security, usability, installability, maintainability and modifiability, and the extent to which the design guidelines in Appendix E have been followed.

All applicable software shall be subject to functional tests. These tests will exercise each system function controlled by the software to verify that the system performs accurately, and performs in accordance with the vendor's specifications and the requirements of the software standards.

The hardware and software tests supplement system-level qualification tests. System-level tests fully exercise the system in an environment similar to that in which the system will be used. They include Physical and Functional Configuration Audits (PCA and FCA). The PCA verifies the configuration, documentation, and support characteristics of the system. The FCA is an exhaustive verification of every system function, and combination of functions, claimed in the vendor's documentation. The test authority also uses the System Operations and System Maintenance Manuals, and verifies their accuracy and completeness during the audit. System-level qualification tests include volume, stress, usability, security, performance, and

recovery tests. These tests may be conducted either as an isolated set of system-level tests, or as part of the audit of the system's functional attributes. They assess the system's response to a range of abnormal conditions initiated in an attempt to compromise the system.

The correctness of software counting logic is also verified during the system-level Functional Configuration Audit. Generic test decks or test data, which represent isolated ballot counting logic scenarios, will be used during this audit (i.e.; multiple test decks for variations in straight party and cross party endorsements will be created and processed).

Acceptance Tests

Section 8 addresses acceptance test requirements. Whereas qualification tests of hardware and software will be performed by an independent test authority prior to state certification, acceptance tests would be conducted by the local jurisdiction, with or without the assistance of independent test authorities, state officials, or outside consultants. The tests will be performed after system procurement, but prior to contractual acceptance.

An adequate acceptance test will demonstrate the integration of hardware and software functions, and the operation of system features and functions, under conditions which realistically simulate primary and general elections in a particular jurisdiction. The jurisdiction will conduct tests to confirm that the delivered systems accurately process ballots, accept valid votes in defined ballot positions, reject overvotes, generate status and error messages and other required audit records, and provide data needed to track and report the vote counting process.

Hardware and software acceptance testing involves functional and performance testing, and a visual examination of the delivered unit(s). Functional tests performed during acceptance testing exercise the required operating features and modes of the delivered units. They are intended to validate that each unit is capable of normal operation. Performance tests are high volume ballot processing tests used to measure compliance with the numerical requirements of the standards (e.g.; reading accuracy processing accuracy, memory stability, etc.). Functional tests are performed on all central count and precinct count units delivered. Performance tests are conducted on all central count systems delivered, but on only a sample of the precinct count units to be installed.

It is recommended that the simulation of vote counting for purposes of acceptance testing involve a configuration of numbers of voters, precinct offices, and candidates, which tests the normal capabilities of the program. Acceptance tests on precinct counters should also include equipment preparation and set-up. Guidelines encouraging acceptance tests prior to contractual acceptance of the equipment may be found in the FEC's voting system management guidelines.

Required Documentation

The standards identify certain records that are to be maintained by the voting system vendor. These are to be submitted by them to the independent test authority conducting the qualification tests. Some of the same documentation will also be needed for state certification review and local acceptance testing.

Required records of hardware and software configuration and development are, as previously stated, described in the hardware and software standards (Subsections 3.1.1 and 4.3, respectively). Documentation of the quality assurance program is discussed in Section 6. Technical data necessary to conduct the system-level qualification tests are discussed in Subsections 7.5.1.2 and 7.5.2.2.

A description of the Technical Data Package (TDP) that must be provided to the test authority as a precondition of qualification is presented in Appendix B. The TDP contains design information to the extent necessary to define the product and its methods of operation. It provides vendor technical and test data that support the functional capabilities and performance levels claimed by the vendor. It also provides an audit trail of software acquisition (e.g.; which items were written in-house, which were procured and modified including descriptions of modifications, and which were procured and not modified).

The TDP must include written instructions and procedures governing operations to be performed by the voter and elections personnel. Maintenance documentation also must be provided in detail sufficient to ensure proper preparation of the system for election use, to facilitate the performance of preventive and corrective maintenance in the field, and to delineate all required supplies, spare parts, and support equipment which should be stocked.

Other Items Relevant to the Standards and Testing Requirements

The appendices contain hardware, software, and test design guidelines; documentation and data retention requirements; testing criteria; ballot specifications; and a glossary of terms. Some of the appendices consist of requirements; others are instructional.

Guidelines for the design of voting system hardware and software are presented in Appendices D and E, respectively. Appendix A lists various publications that are useful in the design and testing of hardware and software. This list includes: American National Standards Institute Standards; Federal Information Processing Standards (FIPS) published by the National Institute of Standards and Technology (formerly the National Bureau of Standards); Electronic Industries Association Standards; Institute of Electrical and Electronics Engineers Standards; IEEE/ANSI Software Engineering Standards; and Military Standards.

The required contents of the Technical Data Package, as stated above, are detailed in Appendix B. Appendix C discusses the data and document retention requirements for punchcard, marksense, and direct recording electronic voting systems.

Appendix F discusses the standards' approach to qualification and acceptance test design. Appendix G specifies the voting system failure criteria established for qualification and acceptance testing. Appendix H delineates mandatory criteria for preparation of a qualification test plan. Appendix I outlines the required contents of a qualification test report. Guidelines for performance tests of P&M systems are presented in Appendix J.

Requirements and specifications for Votomatic ballots are provided in Appendix K. Finally, Appendix L is an informational glossary of terms.

1. Preface

1.1 Purpose

These standards and test specifications establish minimum requirements for punchcard, marksense, and direct recording electronic voting systems and their components. Voting system hardware and software meeting these requirements will have been shown to be reliable, accurate, and capable of secure operation, prior to use in elections.

The standards identify the functional requirements of these systems and components, and the minimum performance, physical, and design characteristics critical to the successful conduct of an election. This establishes industry-wide criteria for minimum levels of system performance in sufficient detail to allow compliance testing.

The standards provide vendors with measurable guidelines for design, logic, and accuracy, and help ensure adequate performance of systems. They provide users with the assurance that any system meeting the standards will perform acceptably; they also provide assistance to users in identifying which products best meet their jurisdiction's needs.

Existing design standards for data processing components, computer programs, supplies and materials should, however, be followed wherever possible, as should standard practices for the design and construction of data processing and telecommunications equipment. Relevant standards and regulations issued by other governmental agencies are incorporated into this standard by specific reference in Appendix A.

1.2 Applicability

The standards may be applied by any entity responsible for the analysis, design, manufacture, procurement, or use of punchcard, marksense, or direct recording electronic voting systems, their subsystems or their components. They apply to all such systems and components first sold or leased after the individual state effective date(s). Systems developed by a third party, such as a voting systems vendor, are covered by these standards, as are software and systems developed in-house by a state or local jurisdiction.

When a new system is contemplated or is being developed that does not follow the general practice for voting systems addressed by these standards, the vendor shall prepare design requirements and specifications for the new system, that conform to the functional requirements and performance levels established by the standards. These specifications shall be submitted to the Federal Election Commission (FEC) for review. During product development, the vendor shall also submit the Technical Data

Package (see Appendix B) to the FEC. The Commission shall negotiate confidentiality agreements to protect the proprietary interests of the system developer. This process will help ensure system acceptability, without adding undue delay in the introduction of new system types or configurations to the market place.

1.2.1 Testing

All equipment and computer programs used in a computerized vote tally system shall be examined and tested to determine their suitability for election use. (See Subsection 7.1.2 for general exemptions.)

Qualification tests shall be performed by an independent testing authority to evaluate logical correctness, accuracy, integrity and reliability. In general, the tests measure the degree to which a system complies with the requirements of these standards. Qualification tests encompass the examination of software and system documentation; tests of hardware under conditions simulating the intended storage, operating, transportation, and maintenance environments; and operational tests verifying system performance and function under normal and abnormal conditions.

Although some of the qualification tests in this document are based on those prescribed in the Military Standards, the test conditions are, in most cases, less severe. This reflects commercial and industrial, rather than military and aerospace, practice.

Subsequent acceptance testing (sometimes called validation testing) shall be conducted to confirm that the delivered voting system hardware and software have the characteristics specified in the procurement documentation, and demonstrated in the qualification tests. Some of the operational tests conducted during systems qualification will be repeated during this testing.

1.2.2 Modifications to Tested Systems

If there are modifications to software or hardware after the system has completed qualification or acceptance testing, further examination and testing is required. Installation of a software package on different hardware than that used during qualification or acceptance testing will require a similar review. The independent test authority will determine what re-qualification tests will be performed. In the instance of software modifications, full software requalification is to be expected.

1.3 Definitions

The standards contain terms which describe design, documentation, and testing attributes of equipment and computer programs. In most cases, the intended sense is that commonly used by computer programmers and operators. In some cases the

usage is more restrictive, and it applies specifically to voting system computer programs. A glossary of these terms is contained in Appendix L. Terms not listed in Appendix L shall be interpreted according to their standard dictionary definitions.

1.3.1 Voting Systems

A voting system is a combination of mechanical, electromechanical or electronic equipment—including the software and firmware required to program and to control the equipment—that is used to cast and count votes. Equipment that is not an integral part of a voting system, but that can be used as an adjunct to it, is considered to be a component of the system.

1.3.2 Punchcard and Marksense (P&M) Voting Systems

A P&M voting system is one which records votes, counts votes, and produces a tabulation of the vote count, using one or more ballot cards imprinted on either or both faces with text and voting response locations. The punchcard voting system records votes by means of holes punched in designated voting response locations; the marksense voting system records votes by means of marks made in the voting response locations.

There are two types of P&M voting systems, classified according to the intended use, and to the manner in which votes are recorded.

P&M Precinct Count Systems tabulate ballot cards at the polling place. These systems are typically used to tabulate ballots as they are cast, and are programmed to print the results of the tabulation after the close of polling. The systems may also provide a means for electronic storage of the tabulation, either in a magnetic medium (on disk or tape) or in a non-volatile semiconductor memory device.

P&M Central Count Systems tabulate ballot cards at a central counting place (or at designated regional sites). Voted ballot cards are typically placed into secure containers at the polling place. After the close of polling, these containers are transported to a central counting place. The systems produce either a printed report of the vote count, a report stored on a magnetic medium or in a semiconductor memory device, or both.

1.3.3 Direct Recording Electronic (DRE) Voting Systems

A DRE voting system is one that records votes by means of a ballot display provided with mechanical or electro-optical devices that can be actuated by the voter, that processes the data by means of a computer program, and that records voting data and ballot images in internal memory devices. It produces a tabulation of the voting data as hard copy or stored in a removable memory device.

1.3.4 Subsystems

All voting systems consist of subsystems which are identified by the functions they perform.

- the **Environment Subsystem**, which consists of all external devices and phenomena which act with or upon the system;

- the **Ballot Definition Subsystem**, which consists of hardware and software required to define ballot layouts for an election, to prepare election-specific software and firmware, and to validate the correctness of all ballot materials and computer programs;

- the **Control Subsystem**, which controls the readying of equipment and software for election use, for pre-election validation testing, and for readiness testing prior to opening the polling place. For precinct count P&M systems and DRE systems, this subsystem governs the opening of the polling place, and the readying of the equipment for use by voters. It also controls the closing of the polling place, the generation of machine-level statements of the vote, and the consolidation of voting data at the precinct level. For central count P&M systems, it controls the validation of ballot formats against the tabulation program, and the generation of precinct-level reports;

- the **Vote Recording Subsystem**, which consists of hardware and software required to detect and record voter choices, permitting legal choices while preventing illegal ones;

- the **Conversion Subsystem**, found only in P&M systems, which consists of all devices and circuitry required to convert voting punches or marks into electronic signals;

- the **Processing Subsystem**, which consists of hardware and software required to accumulate voting data for all candidates and measures within voting machines and polling places, and to consolidate the voting data at a central or regional levels. This subsystem also generates and maintains audit records, detects and disables improper use or operation of the system, and monitors overall system status;

- the **Reporting Subsystem**, which consists of hardware and software required to display status reports and messages, to prepare hard-copy statements of the vote after the polling place has been closed, and to permit the transmission of voting data to a remote location; and

- the **Voting Data Management Subsystem**, which controls the flow and interchange of voting and audit data after extraction from the polling place devices, or after processing precinct data at a central counting place. It consists of hardware and software needed to acquire and consolidate voting data from polling place memory or data transfer devices. The subsystem consolidates this information with data from absentee ballots, manually processed votes, and other data from external sources to produce the official statement of the vote.

2. Functional Requirements

This section contains a functional specification and description of P&M and DRE system components. The requirements specified herein represent acceptable levels of combined hardware and software performance commensurate with overall system requirements for speed, accuracy, reliability, and audit capability.

Functional requirements for P&M and DRE voting system devices include all of the operations necessary to prepare the system for an election, to conduct an election, and, afterwards, to preserve the system data and audit trails.[1]

Pre-voting functions that precede the actual conduct of an election include ballot layout; the installation of general-purpose ballot counting software or firmware; the preparation and installation of election-specific software or firmware; the programming, preparation, and testing of system hardware; and system readiness and verification tests.

Voting functions include all operations conducted at the polling place by voters and officials; operations at central counting places; and the generation of status and output reports. In addition, the election-day operations include support for conducting various readiness and validation tests before and after balloting.

Post-voting functional requirements for P&M and DRE voting systems shall necessarily include means for closing the polling place and for obtaining reports by polling place, by precinct (for central count systems), as consolidated reports, and by machine.

These three functional phases are used to define detailed operating scenarios, within which specific physical and performance requirements of voting systems can be identified. In addition, the overall system requirements relating to security, accuracy and integrity, data retention, and audit capabilities are spelled out.

2.1 P&M System Functions

The functional requirements of P&M systems begin with the preparation of supplies and fixtures required to punch or mark ballots, and with the installation of

1/ Although the following subsystem descriptions might imply that a self-contained piece of hardware is associated with each subsystem, this is not intended.

appropriate software or firmware. They conclude with the production of an output report, either as hard copy, or in a transportable electronic or magnetic storage medium. To ensure compatible interfaces with ballot definition and with generation of an official canvass, this specification includes requirements for aspects of these operations as well.

The general requirements for overall system integrity (Subsections 2.3.1 through 2.3.3) apply to P&M systems and to all operational phases of elections. Functional requirements related to individual election phases are stated in Subsections 2.1.1 through 2.1.3.

P&M voting systems shall perform the following functions as required for the particular system.

2.1.1 P&M Pre-Voting Functions

2.1.1.1 Ballot Definition

P&M systems shall allow for a database that performs automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed upon the ballot.

These systems shall provide a ballot in the form of one or more cards or sheets containing printed information identifying the contests, candidates, and issues. The voter shall make selections by punching a hole or by making a mark in regions (fields) designated for this purpose upon each card or sheet. Alternatively, the information may be printed on an ancillary device into which the ballot card is inserted for punching or marking, and that provides for the alignment of the printed information with the proper voting fields on the ballot.

P&M systems shall be capable of generating sufficient, distinct ballot formats to accommodate requirements for rotation of candidate positions within an office, and requirements for legislative or administrative jurisdictional subsets of a general format.

Ballots generated by these systems shall contain identifying codes or marks uniquely associated with each format.

2.1.1.2 Programming and Software Installation

P&M systems shall provide a means of programming each piece of polling place or central count equipment in accordance with the ballot requirements of the election, and the jurisdiction in which the equipment will be used. The programming means shall include a method for validating the correctness of the program, and of its installation in the equipment or in a programmable memory device.

Such systems shall provide a means to ensure that software (whether nonresident or resident) has been properly selected and installed for the election, and that the software correctly matches the ballot formats that it is intended to process.

2.1.1.3 Equipment Readiness Tests

In P&M systems, each precinct count ballot-counting device, and all central counting equipment, shall contain provisions for verifying its proper preparation for an election, and for verifying that both the hardware and the software are functioning correctly. These tests and diagnostic procedures may be executed manually or automatically, and may allow for operator intervention to validate the proper execution of individually-selected equipment functions.

2.1.1.4 System Readiness Tests

P&M systems shall contain appropriate and necessary provisions for verifying the integration of all system equipment, obtaining status and data reports from each set of equipment, and generating consolidated data reports at the polling place and higher jurisdictional levels.

2.1.1.5 Verification at the Polling Place

P&M precinct count devices shall provide a printed record of the following upon verification of the authenticity of the commands: the election's identification data, the equipment's unit identification, the ballot's format identification, the contents of each active candidate register by office and of each active measure register (showing that they contain all zeros), a list of all ballot fields that can be used to invoke special voting options, and other information needed to ensure the readiness of the equipment, and to accommodate administrative reporting requirements.

Polling place equipment shall permit the use of test ballots to verify the correct interpretation of the ballot format(s) it is programmed to process, and to verify that voting data processing is accurate and reliable. Test data shall be segregated from actual voting data, either procedurally or by hardware/software features.

2.1.1.6 Verification at the Central Counting Place

If a P&M precinct count system includes equipment for the consolidation of polling place data at one or more central counting places, it shall have means to verify the correct extraction of voting data from transportable memory devices, or for the acquisition of such data over secure communication links. Verification shall include the use of security procedures, and communications security devices to be employed during the consolidation of actual voting data, as well as such other tests needed to assure the readiness of the equipment, and to accommodate administrative reporting requirements.

Any P&M system used in a central count environment shall provide a printed record of the following upon verification of the authenticity of the commands: the election's identification data, the contents of each active candidate register by office and of each active measure register (showing that they contain all zeros); and such other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements.

Central count equipment shall permit the use of test ballots to verify the correct interpretation of the ballot format(s) it is programmed to process, and to verify that voting data processing is accurate and reliable. Test data shall be segregated from actual voting data, either procedurally or by hardware/software features.

2.1.2 P&M Voting Functions

2.1.2.1 Opening the Polling Place

P&M systems shall provide a means of verifying that ballotpunching or marking devices are properly prepared and ready for use. All systems shall provide a voting booth or similar facility, in which the voter may punch or mark the ballot in privacy, and secure receptacle for holding voted ballots.

Precinct count equipment shall provide a means of activating the ballot counting device, verifying that the device has been correctly prepared, and allowing the counting of ballots.

2.1.2.2 Candidate and Measure Selection

All P&M systems shall provide for ballots on which are printed labels indicating the names of every candidate, and the titles of every measure on the ballot on which the voter is entitled to vote. Alternatively, these systems may provide ballots to be inserted into a fixture on which such labels are printed. Each label shall indicate the voting field on the ballot that is associated with it.

Such systems shall provide a means by which the voter may directly punch or mark the ballot to register votes. Alternatively, the system may punch or mark the ballot to reflect choices made on an indirect ballot and voter selection display.

The system shall enable the voter to vote for any and all candidates and measures appearing on the ballot, in any legal number and combination to which the voter is entitled.

2.1.2.3 Write-in Voting

A P&M system to be used in any of the states allowing for contest write-in shall provide a means of recording the selection of candidates for any office whose names

do not appear upon the ballot. This means shall consist of the capability for entry of as many names of candidates as the voter is entitled to select for each office.

2.1.2.4 Special Voting Options

Ballot formats in P&M systems shall allow the use of all special options, such as straight party voting, slate voting, and similar methods of selecting more than one candidate by the casting of a single vote. The ballot formats shall permit cross-voting among parties in open, blanket and unitary primary elections, or any other non-standard pattern of voting authorized by the using jurisdictions.

2.1.2.5 Casting a Ballot

In P&M systems, a means shall be provided for the voter to place the voted ballot, or cause it to be placed, into the ballot counting device (precinct count systems), or into a secure receptacle (central count systems). If the voter must leave the voting booth for this purpose, the system shall provide for the privacy of the voted ballot while it is being handled, either by the voter or by a polling place official.

2.1.3 P&M Post-Voting Functions

2.1.3.1 Closing the Polling Place

P&M precinct count devices shall provide a means for preventing the further counting of ballots once the polling place has closed.

2.1.3.2 Obtaining Polling Place Reports

Any P&M system used in a precinct count environment shall provide a means for producing a printed report of the votes counted at the polling place, and for extracting this information from a transportable programmable memory device or data storage medium. Until the proper sequence of events associated with closing the polling place has been completed, the system shall not allow the printing of a report, or the extraction of data. The printed report or electronic memory shall also contain all system audit information required in Section 4.

If more than one unit of vote-counting equipment is used in a polling place, the system shall provide a means for consolidating the data contained in each unit into a single report for the polling place. The consolidation process shall comply with the security and procedural requirements for the system as a whole, and for individual counting devices.

Memory data shall not be altered or destroyed by report generation, and the system shall provide a means for ensuring the integrity and security of data, for at least 6 months after the polls close.

2.1.3.3 Obtaining Precinct Reports by Central Count

Central counting equipment used with P&M precinct count systems shall provide a means for extracting data from transportable memory devices and storage media. This data will be used to produce a printed report of the vote for each precinct.

Central count systems shall provide a means for obtaining a printed report of the centrally-counted votes for each precinct. This printed report shall contain all information required for audits, as defined in Section 4.

Memory data in portable media shall not be altered or destroyed by report generation, and the system shall provide a means for ensuring the integrity of data for a period of at least 6 months.

2.1.3.4 Obtaining Consolidated Reports

P&M systems shall provide a means for consolidating into one report the data from all polling places with that from absentee ballots. This may include consolidation at one or more intermediate levels. The same security and procedural requirements shall be met as apply to the system as a whole, and as apply to individual voting devices.

2.2 DRE System Functions

The functional requirements of DRE systems begin with the creation of a ballot and its matching software or firmware. They conclude with the production of an output report, either as hard copy, or in a transportable electronic or magnetic storage medium. To ensure compatible interfacing with ballot definition, and with generation of an official canvass, this specification includes requirements for aspects of these operations as well.

The requirements for overall systems integrity (Subsections 2.3.1 through 2.3.3) apply to DRE systems generally, and to all operational phases of elections. Functional requirements related to individual election phases are stated in Subsections 2.2.1 through 2.2.3.

2.2.1 DRE Pre-Voting Functions

2.2.1.1 Ballot Definition

DRE voting systems shall allow for the provision for the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed upon the ballot. Such ballots shall comply with the requirements of the statutes and regulations of any jurisdiction in which they are to be used.

The system shall be capable of generating sufficient, distinct ballot formats to accommodate requirements for rotation of candidate positions within an office, and requirements for legislative or administrative jurisdictional subsets of a general format.

Ballots generated by DRE systems shall contain identifying codes or marks uniquely associated with each format.

2.2.1.2 Ballot Installation

DRE systems shall be designed to ensure that the proper ballot is selected for each polling place, and that the format can be matched to the software or firmware required to interpret it correctly.

2.2.1.3 Programming and Software Installation

All DRE systems shall provide a means of programming each piece of equipment to reflect the ballot requirements of the election. This process shall include a means for validating the correctness of the program, and of the program's installation in the equipment or in a programmable memory device.

Such systems shall provide a means to ensure that software (whether resident or nonresident) has been properly selected and installed for any election, and that the software correctly matches the ballot associated with it.

2.2.1.4 Equipment Readiness Tests

Each DRE voting machine or vote recording and data processing device shall contain hardware and software provisions for verifying its proper preparation for an election, and for verifying that both the hardware and the software are functioning correctly. These tests and diagnostic procedures may be carried out manually or automatically, and may allow for operator intervention to validate the proper execution of individually-selected equipment functions.

2.2.1.5 System Readiness Tests

DRE systems shall contain appropriate and necessary provisions for verifying the integration of all system equipment, for obtaining status and data reports from each voting device, and for generating consolidated data reports at the polling place and higher jurisdictional levels.

2.2.1.6 Verification at the Polling Place

All DRE devices shall provide a printed record of the following, upon verification of the authenticity of the commands: the election's identification data, the equipment's unit identification, the ballot's format identification, the contents of each active candidate register by office and of each active measure register (showing that they contain all zeros), all ballot fields that can be used to invoke special voting options, and other information needed to ensure the readiness of the equipment, and to accommodate administrative reporting requirements.

2.2.2 DRE Voting Functions

2.2.2.1 Opening the Polling Place

DRE systems shall provide a means of opening the polling place and readying the equipment for the casting of ballots. This means shall incorporate a security seal, a password, or a data code recognition capability to prevent inadvertent or unauthorized actuation of the poll-opening function. If more than one step is required, it shall enforce their execution in the proper sequence.

2.2.2.2 Party Selection

In a primary election, DRE systems shall provide a voter with means of casting a ballot containing votes for any and all candidates of the party of his choice, and for any and all non-partisan candidates and measures. The voter shall be prevented from voting for a candidate of another party, unless this act is allowed by the statutes and regulations of the jurisdiction using the system.

In a general election, DRE systems shall provide the voter with means of selecting the appropriate number of candidates for any office, and of voting on any measure on the ballot.

2.2.2.3 Ballot Subsetting

If a voter is not entitled to vote for particular candidates or measures appearing on the ballot, the DRE system shall prevent the selections of the prohibited votes.

2.2.2.4 Enabling the Ballot

Once the voter has selected a proper ballot, DRE devices shall provide a means of enabling the recording of votes and the casting of said ballot.

2.2.2.5 Candidate and Measure Selection

DRE voting devices shall provide labels indicating the names of every candidate, and the titles of every measure on the voter's ballot. Each label shall identify the selection button or switch, or the active area of the ballot associated with it.

Such devices shall enable the voter to vote for any and all candidates and measures appearing on the ballot, in any legal number and combination.

The voter shall be able to delete or change his selections before the ballot is cast. A means shall be provided to indicate each selection after it has been made or cancelled.

2.2.2.6 Write-in Voting

A DRE system shall provide a means of recording, if applicable, the selection of candidates whose names do not appear upon the ballot for any office. This means shall consist of the capability for hand-written or, where legally permitted, electronic entry, and subsequent recording, of as many names of candidates as the voter is entitled to select for each office.

2.2.2.7 Special Voting Options

DRE systems shall allow the use of all special options, such as straight party voting, slate voting, and similar methods of selecting more than one candidate, by the selection of the party or slate through a single voter action. The machines shall permit cross-voting among parties in open, blanket and unitary primary elections, or any other non-standard pattern of voting authorized by the jurisdiction in which the system is to be used.

2.2.2.8 Casting A Ballot

DRE devices shall provide a means for the voter to signify that the selection of candidates and measures has been completed. Upon activation, the system shall record an image of the completed ballot, increment the proper ballot position registers, and shall signify to the voter that the ballot has been cast. The system shall then prevent any further attempt to vote until it has been reset or re-enabled by the polling place worker.

2.2.2.9 Public Counter

Each DRE voting device shall be equipped with a counter that can be set to zero prior to opening of the polling place, and that records the number of ballots cast during that particular election. The counter shall be incremented only by the casting of a

ballot. It shall be designed to prevent disabling or resetting by other than authorized persons after the polls close.

The Public Counter shall be visible to all designated polling place officials so long as the device is installed at the polling place.

2.2.2.10 Protective Counter

Each DRE voting device shall be equipped with a counter that records all of the testing and election ballots cast since the unit was built. This counter shall be designed so that its reading cannot be changed by any cause other than the casting of a ballot. It shall be incapable of ever being reset.

The Protective Counter shall be visible at all times when the device is configured for test, maintenance, or election use.

2.2.3 DRE Post-Voting Functions

2.2.3.1 Closing the Polling Place

All DRE devices shall provide a means for preventing further voting once the polling place has closed and after all eligible voters have voted. The means of control shall incorporate a visible indication of system status. The device shall preclude the re-opening once the poll closing has been completed for that election.

2.2.3.2 Obtaining Machine Reports

A DRE system shall provide a means for producing a printed summary report of the votes cast upon each voting device, or for extracting this information from a programmable memory device or data storage medium. Until the proper sequence of events associated with closing the polling place has been completed, the system shall not allow the printing of a report, or the extraction of data. The printed report or electronic memory shall also contain all system audit information required in Section 4.

Data shall not be altered or otherwise destroyed by report generation, and the system shall provide a means for ensuring the integrity and security of data for a period of at least 6 months after the polls close.

2.2.3.3 Obtaining Polling Place Reports

If more than one piece of voting equipment is used in a polling place, the DRE voting system shall provide a means to manually or electronically consolidate the data from all such units into a single report. The same security and procedural requirements

shall be met for this as apply to the system as a whole, and as apply to the individual voting devices.

2.2.3.4 Obtaining Consolidated Reports

DRE systems shall provide a means for consolidating polling place data and absentee results into one report. This may include consolidation at one or more intermediate levels. The same security and procedural requirements shall be met as apply to the system as a whole, and as apply to individual voting devices.

2.3 Overall System Requirements

2.3.1 Security

For **all** types of voting systems, system functions shall be implemented such that unauthorized access to them is prevented and the execution of authorized functions in an improper sequence is precluded. System functions shall be executable only in the intended manner and order, and only under the intended conditions. If the preconditions to a system function have not been met, the function shall be precluded from executing by the system's control logic.

Security provisions for system functions shall be compatible with the procedures and administrative tasks involved in equipment preparation and testing, and in operation by the public in a polling place. If access to a system function is to be restricted or controlled, then the system shall incorporate a means of implementing this requirement.

2.3.2 Accuracy and Integrity

The reliability and quality of memory hardware such as semiconductor devices and magnetic storage media must be high. The overall design of equipment in P&M and DRE systems must provide for the highest possible levels of protection against mechanical, thermal, and electromagnetic (EMI) stress. The system must be able to record accurately each vote and be able to produce an accurate report of all votes cast. The inclusion of control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) shall demonstrate that the system has been designed for accuracy.

Software used in all systems must monitor the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.

P&M systems may rely on the retention of ballots as a redundant means of verifying or auditing election results. (The administrative controls over the distribution and

transport of punchcard and marksense ballots is vital to this redundant level and is addressed in detail under separate cover in the voting systems management guidelines.) As a means of assuring accuracy in DRE machines, the unit must incorporate multiple memories in the machine itself and in its programmable memory devices.

To attain a measure of integrity over the process, the DRE systems must also maintain an image of each ballot that is cast, such that records of individual ballots are maintained by a subsystem independent and distinct from the main vote detection, interpretation, processing and reporting path.[2]

The electronic images of each ballot must protect the integrity of the data and the anonymity of each voter, for example, by means of storage location scrambling. The ballot image records may be either machine-readable or manually transcribed (or both), at the discretion of the vendor.

Both P&M and DRE systems shall include built-in test, measurement and diagnostic software, and hardware for detecting and reporting the system's status and degree of operability.

All systems shall include capabilities of recording and reporting the date and time of normal and abnormal events, and of maintaining a permanent record of audit information that cannot be turned off. For all systems, provisions shall be made to detect and record significant events (e.g.; casting a ballot, error conditions which cannot be disposed of by the system itself, time-dependent or programmed events which occur without the intervention of the voter or a polling place operator).

2.3.3 Data Retention

Both P&M and DRE systems shall contain provisions for maintaining the integrity of memory voting and audit data during an election, and for a period of at least 6 months thereafter. Within the specified design and test ranges, these provisions shall include protection against: the interruption of electronic power; generated or induced electromagnetic radiation; ambient temperature and humidity; the failure of any data input or storage device; and any attempt at improper data entry or retrieval.

Appendix C contains general rules for the 22-month retention of voting system records.

2/ This independent path, if sufficiently simple and being devoid of all the processing complexities of ballot interpretation and vote accumulation, can be tested by an ITA to resolve doubt regarding its logical correctness.

3. Hardware Standards

3.1 Scope

The following sections include Performance Characteristics, Physical Characteristics, Design, Construction, and Maintenance Characteristics for P&M and DRE voting systems. These sections, where applicable, specify minimum values for critical performance and functional attributes involving hardware and software.

The specifications for P&M and DRE systems are organized within the following eight subsystems defined in Section 1:

- Environmental Subsystem, where no distinction is made between requirements for P&M and DRE systems, but requirements for precinct and central count are described;
- Ballot Definition Subsystem, where no distinction is made between requirements for P&M and DRE systems;
- Control Subsystem, where no distinction is made between requirements for P&M and DRE systems;
- Vote Recording Subsystem, where separate and distinct requirements are delineated for P&M and DRE systems;
- Conversion Subsystem, which applies only to P&M systems;
- Processing Subsystem, where separate and distinct requirements are delineated for P&M and DRE systems;
- Reporting Subsystem, where no distinction is made between requirements for P&M and DRE systems, but where differences between precinct and central count systems are obvious; and
- Vote Data Management Subsystem, where no differentiation is made between requirements for P&M and DRE systems.

The performance characteristics include such attributes as ballot reading and handling requirements, system accuracy, memory stability, and the ability to withstand specified temperature, vibration, and shock tests. General requirements

for shelter, electrical supply, compatibility with data networks, punching and marking devices, voting booths, ballot boxes and ballot transfer boxes, communication devices, and printers are also specified.

Reliability, maintainability, availability, and transportability are defined. The standards also include minimum requirements for ballot cards, vote recorders, electromagnetic radiation, product marking, workmanship, interchangeability, safety, and ergonomics.

3.1.1 Hardware Configuration Management

The vendor shall maintain procedures required to identify and document the design and construction of each hardware component, manage changes to the baseline configuration, and record and document revision levels. This shall become part of the Technical Data Package described in Appendix B.

3.2 Performance Characteristics

Performance characteristics for voting systems represent the combined operational capability of both system hardware and software. Accuracy, as measured by bit error rate, and operational failure are treated as two distinct attributes in operational testing (exclusive of code review). During system performance, the desired system-level error rate shall be no more than 1 in 10,000,000. Other performance criteria for subsystem accuracy are presented, as applicable, in sections that follow. Quantitative system reliability shall be measured by the number of unrecoverable failures in a time-based operating test consisting of no less than 163 cumulative hours (with no failures).

All performance requirements contained in Section 3 Hardware shall be met under operating and non-operating conditions.

3.2.1 Environmental Subsystem

The Environmental Subsystem includes shelter, space, furnishings and fixtures, supplied energy, environmental control equipment, and external telecommunications services. The Technical Data Package (TDP) supplied by the vendor shall include a statement of all requirements and restrictions regarding environmental protection, electrical service, telecommunications service, and any other facility or resource required for the installation and operation of the system.

3.2.1.1 Shelter Requirements

All precinct count systems shall be capable of being stored and operated in any enclosed and habitable facility ordinarily used as a warehouse or polling place.

3.2.1.2 Space Requirements

There is no restriction on space allowed for the installation or erection of P&M or DRE systems, except that the arrangement of these systems shall not impede performance of their duties by polling place officials, or the orderly flow of voters through the polling place.

3.2.1.3 Furnishings and Fixtures

Any furnishings or fixtures provided as a part of P&M and DRE systems, and any components which are not a part of these systems but which are used to support its storage, transportation, or operation, shall comply with the design and safety requirements of Subsection 3.4.

3.2.1.4 Electrical Supply

Precinct count systems shall operate with the electrical supply ordinarily found in polling places (120vac/60hz/1). Central count systems shall operate with the electrical supply ordinarily found in central tabulation facilities or computer room facilities (120vac/60hz/1 , 208vac/60hz/3 , or 240vac/60hz/2).

Precinct count systems shall also be capable of operation for a period of at least 16 hours on battery energized power supply. This capability shall include the provision of all power required to enable voting (DRE systems), ballot counting (P&M systems), to display all system status and error messages, and to maintain the contents of program and data memory. This capability does **not** require the provision of illumination of the voting area, nor does it include the production of an output report of the voting data.

3.2.1.5 Environmental Control

Both precinct and central count systems shall withstand storage temperatures ranging from -15 to 150°F (Subsection 7.3.2.5-7.3.2.6), and be capable of operation throughout the temperature range of 40° to 100° (specified in Subsection 7.3.4.2).

3.2.1.6 Data Networks

P&M and DRE voting systems may use a local or remote data network. If such a network is used, then all components of the network shall comply with the environmental requirements for these systems.

3.2.2 Ballot Definition Subsystem

The Ballot Definition Subsystem includes all P&M and DRE hardware and software **and manual procedures** required to accomplish the functions outlined below. The requirements listed below for the Ballot Definition Subsystem illustrate requirements common to the majority of state election laws.

System databases contained in the Ballot Definition Subsystem may be constructed individually, or they may be integrated into one database. They are treated as separate databases herein to identify the necessary types of data which must be handled, and to specify, where appropriate, those attributes that can be measured or assessed for determining compliance with the requirements of this standard.

3.2.2.1 Administrative Database

The subsystem of any P&M or DRE system shall generate and maintain an administrative database containing the definitions and descriptions of political subdivisions and jurisdictions. The environment in which this database is operated shall include all necessary provisions for security and access control, and it shall ensure the security and access control of the other databases in the subsystem.

The two subsidiary databases, enumerated below, may be generated and maintained in any file structure suitable to the requirements of the using jurisdiction. It is the intent of the database hierarchy described herein to ensure that data entry, updating, and retrieval be effectively integrated and controlled. Any structure which provides the required functional capability, security, and privacy is acceptable.

3.2.2.2 Candidate and Contest Database

For each election, the subsystem shall generate and maintain a candidate and contest database, and provide for the generation of properly formatted ballots and software for each P&M and DRE voting device. This database shall interact with the administrative database, to ensure that ballots are properly formatted for each polling place within the jurisdiction.

3.2.2.3 Voter Registration Database

If the subsystem of P&M and DRE systems includes provisions for generating and maintaining a voter registration database, this database shall allow interaction with the administrative database to control, for example, the selection and distribution of correctly formatted sample ballots and absentee ballots.

3.2.2.4 Ballot Generation

In P&M and DRE systems, the subsystem shall provide a software capability for the creation of newly defined elections, for the retention of previously defined formats in that election, and for the modification of a previously defined ballot format.

Such systems shall be designed so as to facilitate the rapid and error-free definition of elections and their associated ballot layouts.

The subsystem shall be capable of handling at least 500 potentially active voting positions, arranged so as to identify party affiliations in a primary election, offices and their associated labels and instructions, candidate names and their associated labels, and issues or measures and their associated text.

The ballot generation capability shall incorporate provisions for rotation of candidate positions within an office, multiple endorsement of candidates by more than one party or body, straight party voting, slate or ticket voting, recall contests, and any other requirements common to the using jurisdiction.

The ballot display may consist of a matrix of rows or columns assigned to political parties or non-partisan bodies, and columns or rows assigned to offices and contests. The display may consist of a contiguous matrix of the entire ballot, or it may be segmented to present portions of the ballot in succession, subject to the requirements of the using jurisdiction.

3.2.2.5 Election Programming

The subsystem in P&M and DRE systems shall provide a facility for the logical definition of the ballot, including the definition of the number of allowable choices for each office and contest, and for the selection of various voting options, in which a single selection causes a vote to be cast for more than one candidate or in more than one office.

The subsystem shall also provide for the logical definition of political and administrative subdivisions, where the list of candidates or contests may vary among polling places, and for the activation or exclusion of any portion of the ballot upon which the entitlement of a voter to vote may vary by reason of place of residence, or other such administrative or geographical criteria.

The subsystem shall generate all required master and distributed copies of the voting program, in conformance with the definition of the ballot for each voting device and polling place. The distributed copies, resident or installable in each voting device, shall include all software modules required to monitor system status and generate machine-level audit reports, to accommodate device control functions performed by

polling place officials and maintenance personnel, and to register and accumulate votes.

3.2.2.6 Ballot Printing or Display

The subsystem shall provide a means of printing or otherwise generating a ballot display, which can be installed in P&M and DRE voting devices for which it is intended. Provisions shall be made to ensure that the allocation of space and the type fonts used for each office, candidate, and contest shall be uniform, and that no active voting position shall be perceived by the voter to be preferred to any other.

3.2.2.7 Ballot Validation

The subsystem of any P&M and DRE system shall provide a facility for generating and executing automated test procedures, to validate both the correctness of election programming for each voting device and polling place, and the correspondence of the ballot display with the installed election program.

3.2.3 Control Subsystem

The Control Subsystem consists of the physical devices, and software (supplemented by administrative procedures) that accomplish and validate the following operations in P&M and DRE systems.

3.2.3.1 Equipment Preparation

The Control Subsystem encompasses hardware and software required to prepare P&M and DRE precinct voting devices, and memory devices for election use. Precinct election preparation includes all operations necessary to install ballot displays, software, and memory devices in each voting device.

The Control Subsystem shall be designed in such a manner as to facilitate the automated validation of ballot and software installation, and to detect errors arising from their incorrect selection or improper installation.

3.2.3.2 Predelivery Testing

Prior to delivery to the polling place, or at any location where diagnostic and maintenance support are available, P&M and DRE voting devices prepared as in the foregoing paragraph shall be subjected to a series of tests.

The Control Subsystem for all precinct count systems includes hardware and software required to support these tests, and to collect data that verifies device readiness. Resident test software, external devices, and special purpose test software connected

to or installed in voting devices to simulate operator and voter functions may be used for these tests, provided that they have been separately tested, and have proven to be reliable verification tools. They must be incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase.

3.2.3.3 Tests at the Polling Place

The Control Subsystem includes hardware and software required to enable opening of the polling place: that is, preparing precinct count P&M and DRE voting devices to accept voted ballots. Prior to opening, each device shall be tested to verify that it is in correct operational status. This test shall include, as a minimum: the production of a diagnostic test record indicating that there are no hardware or software failures, identification of the device and its designated polling place location, that there are no data stored in memory locations reserved for voting data, and that the device is ready to be activated for voting.

3.2.3.4 Opening the Polling Place

The Control Subsystem includes hardware and software required to open the polling place—that is, to allow P&M and DRE voting devices to be enabled for voting. This hardware and software shall include an internal test or diagnostic capability to verify that all of the polling place tests specified in the preceding section have been successfully completed, and if they have not, to disable the device from voting until it has been tested.

3.2.3.5 Enabling a Ballot

The Control Subsystem includes P&M and DRE hardware and software required to enable the casting of a ballot in a general election and, in a primary election, to select the party affiliation declared by the voter, to enable all portions of the ballot upon which the voter is entitled to vote, and to disable any portion of the ballot upon which the voter is not entitled to vote.

3.2.3.6 Error Recovery

The Control Subsystem for P&M and DRE systems includes the hardware and software to enable recovery from a non-catastrophic failure of a device, or from any error or malfunction that is within the operator's ability to correct. Recovery shall mean the restoration of the device to the operating condition existing prior to the error or failure, without loss or corruption of voting data previously stored in the device.

This capability shall also permit resumption of normal operation following the correction of a failure in a memory component, or in a data processing component, including the central processing unit.

For systems other than DRE equipment, checkpointing may be acceptable provided it occurs frequently enough to minimize the amount of re-processing needed to recover from an error condition.

This capability shall also include recovery from any other external condition which causes a voting device to become inoperable, provided that catastrophic electrical or mechanical damage due to external phenomena has not occurred.

3.2.3.7 Closing the Polling Place

In P&M and DRE systems, the Control Subsystem includes hardware and software required to enable closing of the polling place—that is, disabling the casting of additional ballots, and enabling the production of voting data reports. After closing, each device shall be tested to verify that the prescribed closing procedure has been followed, and that the device status is normal.

This test, which may be automated, shall include the production of a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been enabled.

3.2.3.8 Polling Place Reports

If a report of voting data for the polling place is required to be generated at the polling place, the Control Subsystem shall include hardware and software required to produce a report of consolidated data from all P&M and DRE devices in the polling place.

3.2.4 Vote Recording Subsystem

The Vote Recording Subsystem consists of P&M equipment and DRE hardware and software required to record voter choices. There are separate and distinct requirements for P&M and DRE systems.

3.2.4.1 P&M Recording Subsystem

The P&M Recording Subsystem consists of ballot cards or sheets, punching devices, marking devices, frames or fixtures to hold the ballot while it is being punched or marked, and pages or assemblies of pages containing ballot field identification data. It includes compartments or booths, where votes may be conveniently recorded, and that screen the ballot being voted from the view of others. It also includes secure containers for the collection of voted ballots.

3.2.4.1.1 Ballots

Ballot cards or sheets shall meet the requirements of the jurisdictions in which they are used, with respect to formulation, size, thickness, color, watermarks, layout, size and style of printing, arrangement of offices, and size and location of punch or mark fields. Punchcard ballots and some marksense ballots may be counted or recounted on various card readers; therefore, card stock, size, and field layout should conform to the equivalent characteristics of standard Hollerith data processing cards, if this capability is claimed for the system. (See Appendix K for Votomatic punchcard stock specifications.) Printed or punched timing marks may be used for synchronizing the detection of voting punches or marks, provided that they do not appear in any of the data fields of a standard Hollerith card. These limitations do not apply to marksense ballot systems which use paper or oversize card ballots and, in any case, ballots shall be suitable for their intended use, and compatible with the intended card reader.

3.2.4.1.2 Punching Devices

Punching devices shall be suitable for the type of ballot card used. When pre-scored ballot cards are used, the punching device shall consist of a suitable frame for holding the ballot card, and a stylus which the voter uses to remove a scored area of the card to cast a vote. The stylus shall be designed and constructed so as to facilitate its use by the voter, and to minimize damage to other parts with which it comes in contact. It shall incorporate features to ameliorate the effect of skewed insertion, and to ensure that the chad (debris) is completely removed.

3.2.4.1.3 Marking Devices

Marking devices shall be constructed of any materials suitable for the intended use, provided that they meet the reliability and durability requirements of Subsections 3.4.2 and 3.4.3. Marking devices shall be deemed suitable for use if ballots marked by them meet the system performance requirements specified below.

3.2.4.1.4 Frames or Fixtures for Pre-scored Ballots

The frame or fixture for pre-scored cards shall hold the ballot card securely in its proper location and orientation for voting, and incorporate an assembly of ballot label pages that identifies the offices and issues corresponding to the proper ballot format for the polling place where it is used, and that are aligned with the voting fields assigned to them. The frame or fixture shall incorporate a template to preclude perforation of the card except in the pre-scored voting fields, a mask to enable punches only in fields designated by the format of the ballot, and a backing plate for the capture and removal of chad. Any like concept for the positioning of the card, for the association of ballot label information with corresponding punch fields, for the enabling of only those voting fields which correspond to the format of the ballot, for the punching of the fields and for the positive removal of chad, shall be acceptable

provided that the embodiment of the concept shall meet the applicable requirements of this standard. These frames or fixtures are subject to examination for criteria set in Subsections 3.4.2 through 3.4.4, on durability, reliability, and maintainability.

3.2.4.1.5 Frames or Fixtures for Printed Ballots

The frame or fixture for printed ballot cards shall consist of a device into which the card may be placed by the voter, and which positions the card properly. The frame may be of any size and shape consistent with its intended use, and it shall comply with the requirements for design and construction contained in Subsection 3.4.

3.2.4.1.6 Voting Booths

Voting booths, whether integral with the voting system or supplied as components of the voting system, shall comply with the following requirements:

- the booth shall be an enclosure which is integral with or makes provision for the installation of the ballot punching or marking device;
- the structure of the booth shall ensure its stability against movement or overturning during entry, occupancy, and egress by the voter;
- the booth shall provide privacy for the voter, and it shall be designed in such a way as to prevent observation of the ballot by any person other than the voter; and
- the booth shall provide interior space and lighting sufficient to make the process of vote recording convenient and accessible to voters without physical handicap.

If the design and construction of the voting booth is such that it cannot be conveniently used by voters with mobility, dexterity, or visual handicaps, then each polling place shall be equipped with at least one station, meeting the criteria listed above, that can be used by voters with these handicaps.

3.2.4.1.7 Ballot Boxes and Ballot Transfer Boxes

Secure containers shall be provided for the storage and transportation of voted ballots. These containers shall be of a size, shape, and weight commensurate with their intended use. They shall incorporate locks and seals as required by the statutes and procedures of the jurisdictions in which they are used. For precinct count systems, ballot boxes may be integrated with the Conversion Subsystem.

Ballot boxes for both precinct and central count systems may contain separate compartments for the segregation of unread ballots, ballots containing write-in votes,

or any irregularities that may require special handling or processing. In lieu of compartments, the Conversion Subsystem may cause such ballots to be marked with an identifying spot or stripe to facilitate manual segregation.

3.2.4.2 DRE Recording Subsystem

The DRE Recording Subsystem consists of all hardware and software required to detect and record votes, including the logic and data processing functions required to determine the validity of voter selections, to accept and record valid selections, and to reject invalid ones. The subsystem includes the physical environment in which ballots are cast.

3.2.4.2.1 Enclosure

The subsystem for DRE equipment shall include an enclosure that complies with the following requirements:

- the voting device shall be provided with an enclosure, which the voter may enter prior to any other action related to the voting process;
- the structure of the enclosure shall ensure its stability against movement or overturning during entry, occupancy, and egress by the voter;
- the enclosure shall provide privacy for the voter, and it shall be designed in such a way as to prevent observation of the ballot display by any person other than the voter; and
- The enclosure shall provide interior space and lighting sufficient to make the process of vote recording convenient and accessible to voters without physical handicap.

If the design and construction of the voting enclosure is such that it cannot be conveniently used by voters with mobility, dexterity, or visual handicaps, then each polling place shall be equipped with at least one station, meeting the criteria listed above, that can be used by voters with these handicaps.

3.2.4.2.2 Activity Indicator

Each DRE voting device shall be equipped with an audible or visible means for the poll worker of indicating that the device has been enabled for voting, and that a ballot has been cast. This indicator shall be capable of activation or inactivation as required by the using jurisdiction.

3.2.4.2.3 Public Counter

Each DRE voting device shall be equipped with a counter that can be set to zero prior to opening of the polling place, and that records the number of ballots cast during that particular election. The counter shall be incremented only by the casting of a ballot. It shall be designed to prevent disabling or resetting by other than authorized persons after the polls close.

The Public Counter shall be visible to all designated polling place officials so long as the device is installed at the polling place.

3.2.4.2.4 Protective Counter

Each DRE voting device shall be equipped with a counter that records all of the testing and election ballots cast since the unit was built. This counter shall be designed so that its reading cannot be changed by any cause other than the casting of a ballot. It shall be incapable of ever being disabled or reset.

The Protective Counter shall be visible at all times when the device is configured for test, maintenance, or election use.

3.2.4.2.5 Vote Recording

All DRE systems shall contain all mechanical, electromechanical and electronic devices, and software required to detect and record the activation of candidate and contest selections, write-in vote selections, and device controls made by the voter in the process of casting a ballot.

DRE systems shall incorporate multiple memories, both in the voting machine and in its programmable memory device, with polling to detect any discrepancy in the content of individual memories. These systems shall also maintain an electronic or physical image of each ballot, in an independent data path.

This capability shall ensure that recorded ballot images protect the integrity of the data and the anonymity of the voter. The method of recording may include any appropriate encoding or data compression procedure consistent with the regeneration of an unequivocal record of the ballot as cast by the voter.

3.2.4.2.6 Recording Speed

The Vote Recording Subsystem shall be designed so as to permit voters to make selections and cast ballots as rapidly as they are prepared so to do. The average time required to cast the ballot shall not exceed three minutes, with 90 percent of the voter population requiring no more than five minutes, as determined by a test of this subsystem. (See Subsection 7.5.3.)

3.2.4.2.7 Recording Accuracy

DRE systems shall accurately record each vote and ballot cast. Accuracy as here defined means the ability of the subsystem to detect every selection made by the voter, to add permissible selections correctly to the memory components of the device, and to verify the correctness of each of these operations. It also means the ability of the device to preserve the integrity of voting data and ballot images (for DRE machines) stored in memory against corruption by stray electromagnetic emissions, and internally-generated spurious electrical signals.

Recording accuracy may be achieved or enhanced by the incorporation of multiple detection and memory elements that employ device polling techniques. Corrected data errors shall in these instances be logged by the system.

The error rate measured by these criteria shall not exceed one part in one million, as applied independently to the voting data memory and to the ballot image recording devices.

3.2.4.2.8 Recording Reliability

Recording reliability refers to the ability to sustain accuracy during the required operating period. DRE systems shall reliably support the collection and retention of voting data in the voting device and the transmission of voting data among voting devices. The retention, transmission, and collection of voting data shall be error-free for at least 163 hours, as dictated in Subsection 3.4.3 and Appendix F, Subsection F.4.

3.2.5 P&M Conversion Subsystem

The P&M Conversion Subsystem contains all mechanical, electromechanical, and electronic devices required to read the ballot card and to translate its pattern of punches or marks into electronic signals for later processing. This subsystem may be integrated, or it may include one or more components which are not unique to the system, such as a general purpose data processing card reader, or read head, suitably interfaced to the system. This subsystem performs two major functions, ballot handling and ballot reading.

3.2.5.1 Ballot Handling

This function of a P&M Conversion Subsystem consists of the acceptance of a ballot card, its movement through the read station, and transfer into a collection station or receptacle. The speed of ballot handling is not important for precinct count systems into which the voter, or a polling place official, places the ballots one at a time. Speed capabilities for central count systems and their card readers shall be cited by the vendor.

3.2.5.1.1 Outstacking

This requirement does not apply to general purpose card readers. This P&M Conversion Subsystem function refers to the ability of the card readers designed specifically for a voting system to divert cards when they are either not read, or when some condition is detected which requires that the cards be segregated from normally processed ballots, and given special handling according to the operating procedure for the system. Alternatively, such ballots may be marked with an identifying flag to facilitate their identification and removal. Both precinct and central count systems shall provide, as a minimum, the ability to segregate or to place an identifying mark on unprocessed cards, and to segregate or mark cards containing write-in votes, if the candidate's name is entered on the card rather than on a card stub.

If the design of the card reader does not provide for outstacking, then any of the conditions referred to in the preceding paragraph shall cause the card reader to stop, and a status message to be displayed which will permit the operator to remove the card(s) requiring special handling from the remainder of the deck.

3.2.5.1.2 Multiple Feed Prevention

This P&M function refers to the ability of the reader to prevent the feeding of more than one card at a time, or to detect and to provide an alarm indicating the presence of more than one ballot card passing through the read station simultaneously. If multiple feed is detected, the card reader shall halt in a condition that permits the operator to remove the unread cards causing the error, and reinsert them in the card input hopper. The frequency of multiple feeds with ballots intended for use with the system shall not exceed 1 in 5000.

3.2.5.2 Ballot Reading

This P&M function is limited to the conversion of the physical ballot image into an analogous electronic image; the interpretation of the electronic image is the function of the Processing Subsystem. Requirements for the ballot reading function include accuracy and reliability.

3.2.5.2.1 Reading Accuracy

This P&M Conversion Subsystem attribute refers to the inherent capability of the read heads to respond to vote punches or marks, and to discriminate between valid punches or marks and extraneous perforations, smudges, and folds. It includes the conversion of the output of the read head electronic circuitry into digital signals which are transmitted to the Processing Subsystem. Conversion of the output is in response to the presence or absence of a valid voting punch or mark, and not to the presence of signals which fail to meet the detection criteria of a valid punch or mark. Accuracy requirements apply both to the presence and to the absence of a punch or mark in

any active ballot field. That is, valid punches or marks shall be detected, invalid punches or marks shall be rejected, and no detection signal shall be accepted in the absence of a valid punch or mark. Conversion testing shall be performed using all potential ballot positions as active positions. For systems without pre-designated ballot positions, ballots with active position density shall be used. The error rate measured by this criterion shall not exceed one part in one million.

3.2.5.2.2 Reading Reliability

This P&M attribute of the Conversion Subsystem refers to its ability to sustain accuracy during the required operating period. In addition to the reliability life requirements contained in Subsection 3.4.3, the Conversion Subsystem shall reliably read ballots that contain vote marks meeting reasonable criteria for placement, size, and intensity. The rate of rejection of voted ballots shall not exceed 3 percent.

3.2.6 Processing Subsystem

The Processing Subsystem consists of hardware and software required to accumulate voting data for all candidates and measures within voting machines and polling places, and to consolidate the voting data at a central level or levels. This subsystem also generates and maintains audit records, detects and disables improper use or operation of the system, and monitors overall system status. Separate and distinct requirements for P&M and DRE systems are presented below.

3.2.6.1 P&M Processing Subsystem

The P&M Processing Subsystem contains all mechanical, electromechanical, electronic devices, and software required to perform the logical and numerical functions of interpreting the electronic image of the voted ballot, and assigning votes to the proper memory registers. This subsystem also controls the operation of the Conversion and Reporting Subsystems.

3.2.6.1.1 Processing Accuracy

This Processing Subsystem attribute refers to the ability of the subsystem to receive electronic signals produced by vote marks and timing information, to perform logical and numerical operations upon these data, and to reproduce the contents of memory when required, without error. Processing Subsystem accuracy shall be measured as bit error rate, the ratio of uncorrected data bit errors to the number of total data bits processed when the system is operated at its nominal or design rate of processing, in a time interval of 4 hours. The bit error rate shall include all errors from any source in the Processing Subsystem. For all P&M systems, the Maximum Acceptable Value (MAV) for this error rate shall be 1 part in 1,000,000 and the Nominal Specification Value (NSV) shall be 1 part in 10,000,000.

3.2.6.1.2 Memory Stability

P&M memory devices, used to retain control programs and data, shall have demonstrated at least a 99.95 percent probability of error-free data retention for a period of 6 months, under the environmental conditions for operation and non-operation contained in Subsection 3.4.6.

3.2.6.2 DRE Processing Subsystem

The DRE Processing Subsystem contains all mechanical, electromechanical, electronic devices, and software required to process voting data after the polling places are closed.

3.2.6.2.1 Processing Speed

The DRE Processing Subsystem shall operate at a speed sufficient to respond to any operator and voter input without perceptible (less than 250 milliseconds) delay. The time required to extract voting data from a voting device by electronic means shall not exceed one minute. If the consolidation of polling place data is done locally, then the time required to perform this consolidation shall not exceed five minutes for each device in the polling place.

3.2.6.2.2 Processing Accuracy

Processing accuracy is here defined as the ability of the subsystem to process voting data stored in DRE voting devices, or in removable memory modules installed in them. Processing includes all operations on the data performed after the polling places have been closed to consolidate voting data at the polling place. All reports shall be completely consistent; that is, there shall be no discrepancy among reports of voting device data produced at any level.

Consolidated reports containing absentee, provisional, or other voting data shall be similarly error-free. Any discrepancy, regardless of source, shall be resolvable to a procedural error, to the failure of a non-memory device, or to an external cause.

3.2.6.2.3 Memory Stability

DRE memory devices, used to retain control programs and data, shall have demonstrated at least a 99.95 percent probability of error-free data retention for a period of 6 months. Error-free retention may be achieved by the use of redundant memory elements, provided that the capability for conflict resolution or correction is included.

3.2.7 Reporting Subsystem

The Reporting Subsystem contains all mechanical, electromechanical, and electronic devices required for P&M and DRE systems to print audit record entries and results of the tabulation. The subsystem also may include data storage media, and communications devices for transportation or transmission of data to other sites.

3.2.7.1 Removable Storage Media

In all voting systems, items such as programmable read-only memory (PROM), random access memory (RAM) with battery backup, and magnetic tape or disk media, that can be removed from the system and transported to another location for readout and report generation, shall use devices with demonstrated memory stability equal to at least a 99.95 percent probability of error-free retention for a period of 6 months under the environmental conditions for operation and non-operation contained in Subsections 3.4.6 and Section 7.

3.2.7.2 Communication Devices

Devices that may be incorporated in or attached to components of P&M and DRE systems, for the purpose of transmitting tabulation data to another data processing system, printing system or display device, shall not be used for the preparation or printing of an official canvass of the vote unless they conform to an EIA or IEEE standard data interchange and interface structure, and protocol that incorporates some form of error checking.

3.2.7.3 Printers

All printers used to produce reports of the vote count shall be capable of producing alphanumeric headers and election, office and issue labels, as well as alphanumeric entries generated as part of the audit record.

3.2.8 Vote Data Management Subsystem

The Vote Data Management Subsystem for P&M and DRE systems encompasses the management, processing, and reporting of voting data after it has been consolidated at the polling place. It includes hardware and software required to consolidate voting data from polling place data memory or transfer devices, to report polling place summaries, and to process absentee ballots, manually input data, and administrative data from the Ballot Definition Subsystem.

This subsystem includes hardware and software required to generate all output reports in the various formats required by the using jurisdiction.

3.2.8.1 Data File Management

In all voting systems, this subsystem shall include a file management system capable of integrating voting data files with ballot definition files, of verifying file compatibility, and of editing and updating files as required.

3.2.8.2 Data Report Generation

This subsystem for all voting systems shall include report generators for producing output reports at the device, polling place, and summary level, with provision for administrative and judicial subdivisions as required by the using jurisdiction.

3.3 Physical Characteristics

This section covers physical characteristics of both P&M and DRE voting systems, and components which affect their general utility and suitability for election operations.

3.3.1 Size

There are no numerical limitations to the size of any voting system, but it should be compatible with its intended usage.

3.3.2 Weight

There are no restrictions on equipment weight, provided that it is consistent with the environment in which the equipment is to be used. The vendor shall specify the classification of the system, based on the following use environments, so that the proper classification can be used for the hardware transit drop test.

- **Portable** equipment is regularly transported between its operating location and a place of storage. It is typically installed and operated on a table or stand to which it is not permanently affixed, or it is equipped with a collapsible or removal stand or base. It is intended to be hand-carried or handled by one person.

- **Movable** equipment is regularly transported between its operating location and a place of storage. It is typically equipped with a rigid stand or base, with or without wheels or rollers. It is intended to be handled by one or two persons, and handling may require the use of a dolly or lifting mechanism.

- **Fixed** equipment is intended for long-term or permanent placement in its operating location and is not regularly transported to and from a place of storage. It is typically equipped with an integral stand or base. It is

intended to be handled by more than one person, and handling may require the use of a dolly or lifting mechanism.

3.3.3 Transport and Storage

All types of portable equipment shall be provided with a handle or handles to facilitate their handling, transport, and erection or installation. They shall be capable of, or be provided with, a protective enclosure that renders them capable of withstanding impact, shock and vibration loads accompanying surface and air transportation, and stacking loads accompanying storage, as specified in Subsection 3.3.5.

3.3.4 Security

All types of equipment shall incorporate appropriate physical provisions to prevent fraudulent manipulation of the vote recording, counting, and reporting processes. Their design shall preclude unauthorized access to any of the data associated with these processes.

3.3.5 Transportability

All types of voting systems shall be capable of transport by road, rail, or air common carriers.

3.4 Design, Construction, and Maintenance Characteristics

3.4.1 Materials, Processes and Parts

The approach to design shall be unrestricted, and it may incorporate any form or variant of technology which is capable of meeting the requirements and characteristics specified herein. Precinct count systems shall be designed in accordance with best commercial practice for microcomputers, process controllers, and their peripheral components. Central count voting systems and equipment used in a central tabulating environment shall be designed in accordance with best commercial and industrial practice.

The frequency of equipment malfunctions and maintenance requirements shall be reduced to the lowest level consistent with cost constraints.[3] Manufacturers shall prepare an Approved Parts List (APL) for submission as a part of the Technical Data Package. No unit submitted for qualification testing and no production units submitted for sale shall contain parts or components not included in the APL.

3/ Manufacturers are encouraged, but not required, to use MIL-STD 454, "Standard General Requirements for Electronic Equipment," as a guide in the selection and application of materials and parts.

3.4.1.1 Ballot Cards

P&M system ballots that will be processed by general purpose card readers shall utilize card stock, punch configurations, and punch field locations which comply with industry standards for Automatic Data Processing (ADP) supplies and equipment. Ballots intended for use only with their parent system may be of any material and configuration consistent with the requirements of the system. As part of stock finishing, each distinct ballot configuration shall have a unique identification code punched or marked for machine verification. (See Appendix K for ballot stock specifications for Votomatic punchcard ballots.)

3.4.1.2 Ballot Printing

In P&M voting systems, the content and arrangement of printing on ballot cards affects the suitability of systems for election use. Printing shall comply with the regulations and specifications of the using agency. If such do not exist, then the following requirements will apply.

3.4.1.2.1 Punchcard Ballots

Printing on pre-scored cards shall consist of ballot format identification and punch field designation in a type font not smaller than 10 point. Printing on cards that are not pre-scored shall comply with the requirements for Marksense cards.

3.4.1.2.2 Marksense Ballots

Legends and information other than the names of candidates or the statement of issues, shall be printed in a type font not smaller than 12 point. The names of candidates and the titles of issues shall be printed in a type font not smaller than 10 point, and information associated with the name of the candidate or the statement of the issue shall be printed in a type font not smaller than 8 point.

3.4.1.3 Punching Stylus

The stylus for use with automatic punchcard systems shall be suitable for use with the vote recorder and ballots used by the system, and it shall be designed so as to reliably remove chad, and to avoid excessive damage or wear to vote recorder components.

3.4.1.4 Vote Recorder

Vote recorders which utilize ballots to be processed by general purpose card readers shall comply with industry standards for punch configuration and location.

Otherwise, they shall produce punched or marked ballot cards in any manner which is compatible with their parent system.

3.4.2 Durability

The durability of all voting systems and their components refers to their ability to withstand normal use without premature deterioration or wear out. This property can be measured in terms of design life: the period of time throughout which, on the average, individual units will remain serviceable without incurring excessive maintenance costs. Precinct count systems, their components, and associated vote recorders and ballot punches shall have a design life of at least 8 years, and central count systems and their components, at least 12 years.

3.4.3 Reliability

System level reliability for all types of voting systems shall be measured as Mean Time Between Failure (MTBF).[4] Mean Time Between Failure is defined as the value of the ratio of operating time to the number of failures which have occurred in the specified time interval. For the purpose of demonstrating compliance with this requirement, a failure is defined as any event which results in the loss or unacceptable degradation of one or more of the system functions. The MTBF demonstrated during qualification testing by the procedure of Section 7 shall be at least 163 hours.

3.4.4 Maintainability

The design characteristics of all voting equipment determine the ease with which maintenance actions can be performed. Maintenance actions include all scheduled and unscheduled events which are performed to:

- determine the operational status of the system and its elements;
- adjust, align, or service circuits and components;
- replace a circuit or component having a specified operating life or replacement interval;
- repair or replace a circuit or component which exhibits an undesirable predetermined physical condition or performance degradation;
- repair or replace a circuit or component which has failed; and

4/ Reliability can best be ensured by selecting electronic and electromechanical parts according to criteria spelled out in MIL-STD 454 and NASA 975G.

- verify the restoration of a circuit, a component, or the system to operational status.

Qualitative measures of maintainability include

- ease of access to internal components;
- the presence of labels and the identification of test points;
- the provision of built-in test and diagnostic circuitry or physical indicators of condition;
- the ease with which adjustment and alignment can be performed; and
- the presence of easily disconnected electrical and mechanical interfaces which facilitate the removal and replacement of circuits and components.

Quantitative measures of maintainability include the following indices.

3.4.4.1 Mean Time to Repair (MTTR)

MTTR is the average time required to perform a corrective maintenance task. Corrective maintenance task time is active repair time, excluding logistic or administrative delays. Corrective maintenance may consist of substitution of the complete device or component, as in the case of precinct count and some central count systems, or it may consist of on site repair. MTTR attributes of systems and components shall be sufficient to achieve, in combination with their MTBF, the required availability.

3.4.4.2 Maximum Repair Time (Mmax)

The frequency distribution of active repair times shall be such that, for precinct count systems, there is less than a 1 percent probability, and for central count systems less than a 5 percent probability, that an unscheduled maintenance action shall require more than 1.0 hour to complete. In the event that this requirement is not met for any component or for the complete system, then an equivalent component or system shall be provided, and placed in a ready standby state throughout the operating period.

3.4.4.3 Maintenance Ratio (MR)

Maintenance Ratio is the ratio of total maintenance man-hours (MMH) to total operating hours (OH). MMH shall equal the sum of the scheduled and unscheduled maintenance man-hours spent on all units of equipment in the system, and OH shall include the nominal time of system operation, including the time required to prepare

the system for an election, and the time required to conduct post-election operations. The maintenance ratio for all types of systems shall not exceed 0.25 MMH/OH.

3.4.5 Availability (Ai)

Availability is the probability that the system will respond to an operational demand. It is the ratio of the time during which the system is operational (up time) to the total time period (up time plus down time). Inherent availability (Ai), is based upon MTBF and active repair time (MTTR), that is:

$$Ai = (MTBF)/(MTBF + MTTR)$$

System availability as here defined shall be at least 0.99.

3.4.6 Environmental Conditions

Environmental conditions applicable to the design and operation of voting systems consist of the following categories: the natural environment, which includes the effects of temperature, humidity, and atmospheric pressure; the induced environment, including both the effects of use, such as the proper and improper operation and handling of the system and its components during the election processes, and the effects of transportation and storage; and the electromagnetic signal environment, including exposure to and the generation of radio frequency energy.

All voting systems shall be designed to withstand the environmental conditions contained in the appropriate test procedure of Section 7.

3.4.7 Electromagnetic Radiation

Voting systems of all types shall comply with the Rules and Regulations of the Federal Communications Commission, Part 15 "Radio Frequency Devices," Subpart J, "Computing Devices." Voting systems of any type shall be considered "Class B" computing devices, as defined therein.

3.4.8 Product Marking

All voting system components shall be identified by means of a permanently affixed nameplate or label containing the name of the manufacturer or vendor, the name of the device, its part or model number, its revision letter, and its serial number. Power requirements, if any, shall also be specified.

A separate data plate containing a schedule for and list of operations required to service or to perform preventive maintenance on the component shall be similarly affixed.

Advisory caution and warning instructions to assure safe operation of the equipment and to avoid exposure to hazardous electrical voltages and moving parts shall be provided at all locations where operation or exposure may occur.

3.4.9 Workmanship

Workmanship standards for P&M and DRE voting systems shall meet or exceed standard commercial and industrial practice. Manufacturers of all voting systems and components shall adopt additional practices and procedures, if necessary, to ensure that their products are free from damage or defect that could make them unsatisfactory for their intended purpose. Manufacturers are referred to the Hardware Design Guidelines in Appendix D.

3.4.10 Interchangeability

Manufacturers of P&M and DRE voting systems and components, shall utilize design and construction features that maximize interchangeability, thereby facilitating maintenance and the incorporation of product revisions or improvements.

3.4.11 Safety

All voting systems and their components shall be designed so as to eliminate hazards to personnel, or to the equipment itself. Defects in design and construction, which can result in personal injury or equipment damage, must be detected and corrected before voting systems and components are placed into service. Equipment design for personnel safety shall be equal to or better than the appropriate requirements of the Occupational Safety and Health Act (OSHA), as identified in Title 29, part 1910, of the Code of Federal Regulations. Additional sources for guidance in the elimination of safety hazards are contained in Appendix D.

3.4.12 Human Engineering

Both P&M and DRE voting systems and components shall be designed and constructed so as to simplify and facilitate the functions required, and to eliminate the likelihood of erroneous stimuli and responses on the part of the voter or operator. Guidance in the overall achievement of this objective is contained in Appendix D. Other specific requirements are contained in the following paragraph.

3.4.12.1 Controls and Displays

In P&M and DRE systems, all controls used by the voter or equipment operator shall be conveniently located, shall use designs that are consistent with their functions, and shall be clearly labelled. Instruction plates shall be provided, if they are necessary to avoid ambiguity or incorrect actuation.

Information or data displays shall be large enough to be readable by a person with normal eyesight, from a normal operating distance, and with any level of ambient lighting suitable for equipment operation.

Status displays shall meet the same requirements as data displays, and they shall also follow conventional industrial practice with respect to color. Green, blue, or white displays shall be used for indications of normal status; amber indicators shall be used to indicate warnings or marginal status, and red indicators shall be used to indicate error conditions or equipment states that may result in damage, or in hazards to personnel. Unless the equipment is designed to halt under conditions of incipient damage or hazard, an audible alarm shall also be provided.

4. Software Standards

4.1 General

The requirements of this section are intended to ensure that the overall objectives of logical correctness, system integrity, reliability, and accuracy are achieved. In general, these formal requirements affect the control of ballot counting, vote processing, the creation of an unalterable audit trail, and the generation of output reports. Although this section emphasizes software, the described standards also influence hardware considerations. These standards are intended to guide the design of software written in any of the programming languages commonly used for mini-computer and microprocessor systems. They are not intended to preclude the use of other languages and environments, such as those that exhibit "declarative" structure, "object-oriented" languages, "functional" programming languages, or any other combination of language and implementation that provides appropriate levels of performance, testability, reliability, and security.

Compliance with the requirements of these software standards shall be assessed by means of code examination of all ballot tally application software, as well as other formal tests. (Code inspection of any ballot preparation-layout modules will not usually be undertaken.) Some of the analysis and test requirements do not depend upon the design and coding of the software, but others do. The use of proven and widely acceptable software design methods facilitates the necessary analysis and testing.

4.2 Software Design and Coding Requirements

The ballot counting software shall be designed in a modular fashion and shall not be self-modifying. Modular programs consist of code written in relatively small and easily identifiable sections, with each unit having a single entry point and a single exit point. Each module shall have a specific function that can be tested and verified more-or-less independently of the remainder of the code. Appendix E contains numerical guidelines for program modules.

It is preferable, but not mandatory, that a high level programming language be used for that segment of the ballot tabulation software associated with the logical and numerical operations on vote data. Such languages include, but are not limited to: Pascal, COBOL, Fortran, and C. The preferential use of high level language for logical operations does not preclude the use of assembly language for hardware-related segments, such as device controllers and handler programs. Also, operating system software may be designed in assembly language.

High level languages support another recommended design concept: structured programming. Structured programs embody constraints on module entry and exit conditions, and on the manner in which internal logical tests and operations are implemented. This minimizes the likelihood of structural and logical programming errors.

Other preferred coding practices and software characteristics are presented in Appendix E.

4.3 Configuration Management

The vendor shall maintain procedures required to identify and document the physical and functional characteristics of each software and firmware unit, manage changes to these characteristics, record and document the processing of changes, and identify the configuration and characteristics of all released versions.

The vendor shall provide an audit trail of software acquisition. This shall include documentation of which software items were written in-house, which were procured and modified including descriptions of the modifications, and which were procured and not modified. The vendor shall also provide a certification that procured items were obtained directly from the manufacturer.

The vendor shall also maintain documentation of the software development process, including all records of module and functional tests. This documentation is an important element in analyzing and testing; if developmental data is not preserved, it cannot be recreated.

All of this information shall become a part of the Technical Data Package described in Appendix B, to be submitted as a precondition for qualification. Recommended formats for system documentation are contained in the Appendix, and include both technical and user items.

All software altered from the baseline configuration submitted for qualification shall be subject to retest at the discretion of the independent test authority. No compiler(s) other than those specified as part of the technical data submitted for the Physical Configuration Audit shall be used for testing or election-day processing.

4.4 Data Quality Assessment

Provision shall be made for real-time monitoring of system status and data quality. Methods of assessment shall be determined by the vendor. Implementation options include but are not limited to: (1) hardware monitoring of redundant processing functions which are carried out in parallel or serially; and (2) statistical assessment and measures of system operation.

Measurement of the relative frequency of entry to program units, and the frequency of exception conditions, should be included as part of the quality assessment.

4.5 Vote Recording Accuracy and Integrity

The system must be able to record accurately each ballot cast by the voter, and able to produce an accurate report of all votes cast. The inclusion of control logic and of data processing methods incorporating parity and check-sums (or other equivalent error-detection and error-correction methods) shall demonstrate that the system has been designed for accuracy.

Software used in all systems must monitor the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected. If the total number of corrected errors exceeds a predetermined threshold, or if errors of any one type occur repeatedly, then the operation of the affected device must be suspended until the condition generating the errors has been corrected. Any uncorrectable error must result in an immediate halt, and provide an appropriate message to the voter or polling place official.

P&M systems may rely on the retention of ballots as a redundant means of verifying election results. As a means of assuring accuracy in DRE machines, the unit must incorporate multiple memories in the machine itself and in its programmable memory devices. To attain a measure of integrity over the process, DRE systems must also maintain images of each ballot that is cast, such that records of individual ballots are maintained by a subsystem independent and distinct from the main vote detection, diagnostic, processing and reporting path.[5]

The stored images of each ballot must protect the integrity of the data and the anonymity of each voter, by such means as storage location scrambling. The ballot image records may be either machine-readable or manually transcribed (or both), at the discretion of the vendor.

5/ This independent path, if sufficiently simple and being devoid of the many processing complexities of ballot interpretation and vote accumulation, can be tested by an ITA to verify its logical correctness.

The DRE firmware instructions shall contain necessary logical instructions to determine correct recording of each and every candidate selection made by the voter to the appropriate memory registers and tables. In the case of a partially-voted ballot, deliberate undervoting by a voter will be permitted; such undervoting will be validated by machine determination that particular candidate selections have not been made. In those cases where a selected candidate is not recording correctly upon casting of the ballot, the DRE equipment shall generate an error signal and automatically stop operation of the machine until the problem is resolved.

In other words, after every ballot is cast, a reconciliation of the sum of selections and undervotes is needed. The undervotes shall not be generated as a default but as the result of scanning the ballot as it is cast.

4.6 Data and Document Retention

All systems shall contain provisions for maintaining the integrity of voting and audit data during an election, and for a period of at least 6 months thereafter, a time sufficient in which to resolve most contested elections. These provisions shall include protection against the failure of any data input or storage device, and against any attempt at improper data entry or retrieval.

Prior to system qualification, each vendor shall submit to the Federal Election Commission a written request for information regarding the types and respective formats of election specific data that must be retained by the user jurisdictions for the 22-month period. The Commission will, in turn, request a formal ruling from the Election Crimes Branch of the Department of Justice (DOJ). For each system, the vendor shall present detailed operational characteristics, such that DOJ can rule on specific data and document items and their preferable media (manual and/or electronic format) that are to be retained for the auditability and reconstruction of the election process.

4.7 Ballot Interpretation Logic

There are significant variations among the election laws of the 50 states with respect to methods and features of voting, and with respect to ballot formats. If a voting system is offered for qualification at the national level, the following characteristics of its ballot interpretation logic (and their variations) will be tested during qualification. The vendor shall identify any of the following items and variations which cannot be accommodated by the system:

- closed and open primary elections
- partisan and non-partisan offices
- straight party voting options
- slate or group voting options

- cross-party endorsement
- primary presidential delegation nominations
- rotation of names within an office
- recall issues, with options
- reassembly of multi-card ballots
- split precincts
- vote for N of M
- write-in voting
- overvotes and undervotes
- totally blank ballots

4.8 System Audit Requirements

Election audit trails provide the supporting documentation for verifying the correctness of the reported results. They present a concrete, indestructible archival record of all system activity related to the vote tally. They are, of course, essential for public confidence in the accuracy of the tally, for recounts, and in the event of litigation.

The following audit trail requirements are based on the premise that system-generated creation and maintenance of audit records reduces the chance of human error. Since most of the audit capability is automatic, the operator has less information to track and record, and is less likely to make mistakes or omissions.

The sections that follow present operational requirements and audit records critical to acceptable performance and reconstruction of an election. Four types of audit records are distinguished, tracking: the preparation of ballot formats and election specific software; tests of system readiness; the actions of individuals and machines during election processing and the resulting vote tally data. Optional in-process audit records and vote tally records that may contribute to increased levels of public confidence are listed in Appendix E.

The requirements for all system types, both precinct and central count, are described in generic language. Because the actual implementation of specific characteristics may vary from system to system, it is the responsibility of the vendor to describe each system's characteristics in sufficient detail that test authorities and system users can evaluate the adequacy of the system's audit trail. This description should be incorporated in the System Operating Manual, which is part of the Technical Data Package.

Also part of the election audit trail, but not covered in these technical standards, is the documentation of such items as ballots delivered and collected, administrative procedures for system security, pre-election testing of voting systems, and maintenance performed on voting equipment. A discussion of these records will be presented

in management guidelines produced by the Federal Election Commission in the future.

4.8.1 Operational Requirements

Audit records shall be prepared for all phases of elections operations. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. Primary emphasis is placed upon audit records of the ballot preparation and election definition phase, of system readiness tests, and of voting and ballot-counting operations. The software shall activate the logging and reporting of audit data as described in the following sections.

4.8.1.1 Time, Sequence, and Preservation of Audit Records

The timing and sequence of audit record entries is as important as the data contained in the record. Except where noted, provisions shall be made for the creation and maintenance of a real-time record. The purpose of the real-time record is to provide the operator or precinct official with continuous updates on machine status. This information allows effective operator intervention during an error condition, and contributes to the reconstruction of election-related events necessary for recounts or litigation.

All systems shall incorporate a real-time clock as part of system hardware. It should maintain an absolute record of the time and date or a record relative to some event whose time and data are known and recorded. All audit record entries shall include the time-and-date stamp.

The audit record shall be in use whenever the system is in an operating mode; this record shall be available at all times, though it need not be continually visible. The generation of entries shall not be terminated or interfered with by program control, or by the intervention of any person. The physical security and integrity of the record shall be maintained at all times.

Once the system has been activated for ballot processing, the contents of the audit record shall be preserved during any interruption of power to the system until processing and data reporting have been completed.

A separate printer is not required for the audit record, and the record may be produced on the standard system hardcopy output device if the following conditions are met:

- the generation of audit trail records does not interfere with the production of output reports;

- the entries can be identified so as to facilitate their recognition, segregation, and retention; and

- the physical security of the audit record entries can be ensured.

4.8.1.2 Error Messages

Error message entries shall be made and reported as they occur. Except for error messages which require resolution by a trained technician, all other error messages requiring intervention by an operator or precinct official shall be displayed or printed unambiguously in easily understood language text, or by means of other suitable visual indicators.

When numerical codes are used for trained technician maintenance or repair, the text corresponding to the code shall be self-contained, or an instructional sheet shall be affixed inside the unit device. This is intended to reduce inappropriate reactions to error conditions, and to allow for ready and effective problem correction.

The message cue for all systems shall clearly state the action to be performed in the event that voter or operator response is required. System design shall ensure that erroneous responses will not lead to irrecoverable error. Nested error conditions shall be corrected in a controlled sequence such that system status shall be restored to that initial state existing before the first error occurred.

4.8.1.3 Status Messages

Depending on their nature, status messages may or may not become part of the real-time audit record. Non-critical status messages need not be displayed at the time of occurrence.

Latitude in software design is necessary, so that consideration can be given to various user processing and reporting needs. The user may require some status and information messages to be displayed and reported in real-time; other messages, which do not require operator intervention, may be stored in memory, to be recovered after ballot processing has been completed.

Depending on the critical nature of the message, and the particular jurisdiction's needs, status messages shall preferably be displayed and reported by suitable, unambiguous indicators or English language text. It is acceptable to display non-critical status messages which do not require operator intervention by means of numerical codes, for subsequent interpretation and reporting as unambiguous text.

4.8.2 Audit Record Data

The audit record provisions listed in the following subsections are considered essential to the complete recording of election operations and reporting of the vote tally. This list of audit records may not reflect idiosyncracies of some systems; therefore, vendors shall supplement it with information relevant to the operation of their specific systems.

4.8.2.1 Pre-election Audit Records

During election definition and ballot preparation phases, an audit log shall be maintained of completion of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates. These data are required to verify the election-specific database has been correctly prepared and maintained throughout subsequent modifications to the baseline format.

The pre-election audit log shall include manual data maintained by election personnel, samples of all final ballot formats, and the ballot preparation edit listings associated with them.

4.8.2.2 System Readiness Audit Records

Prior to the initiation of ballot counting, software shall be able to verify hardware and software status through an audit record. This readiness audit record shall include the identification of the software release, the identification of the election to be processed, and the results of software and hardware diagnostic tests. In the case of systems used at the polling place, the record shall include the polling place's identification.

The ballot interpretation logic capability shall test ballot formats to be processed. Such tests shall verify the allowable number of votes for an office or issue, the combinations of voting patterns permitted or required by the using jurisdiction, the inclusion or exclusion of offices or issues as the result of multiple districting within the polling place, and any other characteristics that may be peculiar to the jurisdiction, the election, or the polling place's location.

For P&M systems, this readiness audit capability shall evaluate the accuracy of the ballot reader and the arithmetic-logic unit. It shall allow the processing, or simulated processing, of sufficient test ballots to provide a statistical estimate of processing accuracy.

For all systems, the software shall ensure non-contamination of voting data through checks of all data paths and memory locations to be used in actual vote recording; upon the conclusion of the tests, the software shall provide evidence in the audit record that the test data have been expunged.

4.8.2.3 In-Process Audit Records

In-process audit records consist of data documenting precinct and central count system operation during diagnostic routines and the casting and tallying of ballots. At a minimum, the in-process audit records shall contain the following items, which apply to all systems, except as otherwise noted:

- Machine generated error and exception messages to ensure that successful recovery has been accomplished. Examples include, but are necessarily limited to:

  (a) the source and disposition of system interrupts resulting in entry into exception handling routines;

  (b) all messages generated by exception handlers;

  (c) the identification code and number of occurrences for each hardware and software error or failure;

  (d) notification of system log-in or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing;

  (e) for P&M systems, an event log of any ballot-related exceptions such as:

    (i) quantity of ballots that are not processable;

    (ii) quantity of ballots requiring special handling;

    (iii) in a central count environment, quantity and identification number of aborted precincts; and

  (f) other exception events such as power failures, failure of critical hardware components, data transmission errors, or other type of operating anomaly.

- Critical system status messages other than informational messages displayed by the system during the course of normal operations. These items include, but are not limited to:

  (a) diagnostic and status messages upon startup;

  (b) the "zero totals" check conducted before opening the polling place or counting a precinct centrally;

(c) for P&M systems, the initiation or termination of card reader and communications equipment operation; and

(d) for DRE machines the event (and time, if available) of enabling/casting each ballot (i.e.; each voter's transaction as an event). This data can be compared with the public counter for reconciliation purposes.

- Non-critical status messages that are generated by the machine's data quality monitor or by software and hardware condition monitors, though this information is not required in real-time and may, instead, be reported in log form. For example, a cumulative or summary record of data read-write-verify, parity, or check-sum errors and retries is required: the intent is to gauge the accuracy of the ballot data and adequacy of the system in monitoring and detecting system processing errors.

- System generated log of all normal process activity and system events that require operator intervention, so that each operator access can be monitored and access sequence can be constructed.

4.8.2.4 Vote Tally Data

In addition to the audit requirements spelled out in the previous subsections, there are other election-related data essential for reporting results to interested parties, the press, and the voting public. This data is vital to verifying an accurate count. Meeting these reporting requirements depends on the ability of the software to obtain data concerning various aspects of vote counting, and to produce reports of them on a printer or at a terminal.

At a minimum, vote tally data shall include:

- Number of ballots cast, by each ballot configuration/type.

- Candidate and measure vote totals for each contest.

- The number of ballots read within each precinct, by type, including totals for each party in primary elections.

- For P&M systems, the total number of ballots both processed and unprocessable; and if there are multiple card ballots, the total number of cards read.

- Separate accumulation of overvotes and undervotes for each race or issue (no overvotes would be indicated for DRE devices).

5. Security

5.1 General

It is recognized that no security system is capable of defeating all conceivable or theoretical threats. The computerized tally, like the voting process, must accommodate some degree of public scrutiny and access, but fail-safe measures cannot be guaranteed. Vendors and election authorities must therefore do everything that prudence dictates, and that the available resources permit, to institute a security program. The overall objectives of this program are: to identify potential threats, to conduct a risk analysis, to develop appropriate counter-measures, and to assign responsibilities for execution of a security plan.

The ultimate goal of the security analysis is to obtain an acceptable level of confidence in the integrity, reliability, and inviolability of the entire election process. To accomplish this, vendors and election authorities must:

- maintain controls which can ensure that accidents, inadvertent mistakes, and errors are minimized;
- protect the system from intentional, fraudulent manipulation, and from malicious mischief; and
- identify fraudulent or erroneous changes to the system.

The system design and logic must include access protection schemes, validation routines, self-diagnostics, error recovery routines, restart and logging capabilities, and other security measures to protect vital parts and operating states, as appropriate. Security provisions for system functions shall be compatible with the procedural and administrative environment typical of equipment preparation and testing, and shall be compatible with operation by the public in a polling place. If access to a system function is to be restricted or controlled, then the system shall incorporate a means of implementing the access control requirement.

5.1.1 Scope of Testable Security Standards

Security encompasses a broad range of safeguards external to the actual computer system, as well as security measures embedded in the hardware, software, and operating systems. These include:

- administrative and management controls (data processing and election management);
- operational procedures (i.e., effective password management);
- physical facilities and arrangements;
- organizational responsibilities and personnel screening;
- communications; and
- technical hardware and software.

The following requirements in this section are tied to the technical aspects of hardware, software, and communications security that can be readily examined, assessed, and tested during qualification. Reference is also made to vendor and user responsibilities.

Excluded from detailed discussion in this document are recommended jurisdiction-specific practices concerning administrative and management controls, internal security procedures, physical facilities, organizational responsibilities, and pre-election day testing. Such recommendations on accepted practice will be contained in the FEC management guidelines.

Audit trail requirements are covered in Subsection 4.8 of the Software Standards section. As an integral part of software capability, computer-generated audit controls provide inherent system security.

5.2 Initiation of Security Plan

The using jurisdiction shall be responsible for initiating a security program and policies covering: physical protection of facilities, data and communications access controls, internal procedural security, contingency plans, and standards for programming, acceptance testing, audit trails, and documentation.

5.3 Access Control

All software (including firmware) for all voting systems shall incorporate measures to prevent access by unauthorized persons, and to prevent unauthorized operations by any person. Unauthorized operations include, but are not limited to: modification of compiled or interpreted code, run-time alteration of flow control logic or of data, and abstraction of raw or processed voting data in any form other than a standard output report by an authorized operator.

The vendor shall provide a penetration analysis relevant to the operating states of the system, and to its environment. This analysis shall cover the individual use of program units, the planned or inadvertent sharing of program units, and the resulting transitivity relationships. It shall identify all entry points and the methods of attack to which each is vulnerable. Such penetration analysis will be subject to strict confidentiality and non-disclosure by the test authority. For security reasons, the penetration analysis shall not be routinely distributed to the jurisdictions that program elections. The penetration analysis, however, will be part of the escrow deposit.

5.3.1 Access Control Policy

The general features and capabilities of the access policy shall be specified by the vendor. Such generic capabilities might well include software access controls, hardware access controls, effective password management, the protection abilities of a particular operating system, and the general characteristics of supervisory access privileges.

The using jurisdiction in charge of voting system operations shall be responsible for defining the specific access policies applying to each election, and for defining any variations of these resulting from use of the system in more than one environment.

The access control policy shall identify all persons to whom access is granted, and the specific functions and data to which each holds authorized access. If an authorization is limited to a specific time, time interval, or phase of the voting or counting operations, this limitation shall also be specified.

The access control policy shall not affect the ability of a voter to record votes and submit a ballot, but the policy shall preclude voter access to all other physical facilities of the vote-counting processes.

5.3.2 Access Control Measures

Access control measures shall be designed to permit access to system states in accordance with the access policy, and to prevent all other types of access. These measures may include: the use of data and user authorization, program unit ownership and other region boundaries, one-end or two-end port protection devices, security kernels, computer-generated password keys, special protocols, message encryption, and controlled access security modems (see NIST Special Publication 500-137, *Security for Dial-Up Lines*).

Control methods shall also be defined to preclude unauthorized access to the access control system itself.

5.4 Equipment and Data Security

There are two areas of concern which must be addressed by security plans: disruption of the voting process, and corruption of voting data. Disruption of the process, such as the interruption of voting and vote counting, or the recoverable destruction of program and data files, may be minimized by controlling physical access to the system. Corruption of voting data may be addressed by the use of data encryption techniques, and by the control of information flow.

5.4.1 Physical Security Measures

The sensitivity of a voting system to disruption or corruption of data depends, in part, on the physical location of equipment and data media, and on the establishment of secure telecommunications among various locations.

Disruption of voting and vote counting results most often from a physical violation of one or more areas of the system thought to be protected. Security procedures shall, therefore, address physical threats and the corresponding means to defeat them.

For polling place operations, procedures shall be developed and enforced to anticipate and counter acts of vandalism, civil disobedience, and similar obstructionist tactics. The procedures shall allow the immediate detection of tampering with the ballot punching and marking devices, and with precinct ballot counters. If a telecommunications channel links the polling place to a central computer location, then a procedure to control physical access to the link is required.

Similar procedures shall be developed and enforced in a central counting environment. These shall include physical and procedural controls on the handling of ballot boxes, on the preparation of ballots for counting, on counting operations, and on data reporting.

5.5 Software and Firmware Installation

If software is resident in the system as firmware, retesting of every device to validate each ROM is necessary prior to the start of elections operations. This is to provide assurance that the software is intact in its intended form and that its integrity and security have not been breached. Therefore, restrictions shall be imposed on this residency and the firmware or the equipment containing it shall be maintained in a secure environment.

To prevent alteration of executable code, no software or firmware shall be permanently installed or resident in the system unless it is required that the user provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.

The system bootstrap, monitor, and device-controller software may be resident permanently, provided that this firmware has been shown to be inaccessible to actuation or control by any means other than the authorized initiation and execution of the vote-counting program, and its associated exception handlers.

After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible. This requirement is intended to prevent alteration and recompilation of the program. For example, for ballot-counting software operating in a multi-user environment, installation shall consist of a bootable module that permits only the execution of the application program and does not allow exit to the operating system generally.

5.6 Communications and Data Transmission

In addition to the security requirements contained in Subsections 5.1 through 5.5, the security of data transmission must be assured. Therefore, communications links used for system control and data input/output are subject to the same security requirements governing access to any other system hardware, software, and data function.

The objectives of protecting data integrity, and of precluding unauthorized access to it, deal with two potential threats. First, a means must be provided to ensure that errors, whether deliberate or inadvertent, are prevented—or, at least, are detected if they occur. Parity checks, check-sums and ECC (error detection and correction codes) are examples of applicable data integrity techniques; other relevant techniques include various forms of data encryption that make the interpretation of intercepted data difficult, and that are capable of detecting corrupted data. See NIST FIPS Pubs. 31, 113, and Special Publication 500-137. A means must also be provided to detect the presence of an intrusive device, such as a wiretap or electromagnetically-coupled pickup, and to prevent the leakage of data from an authorized process (such as a telecommunications transmission) to an unauthorized recipient.

5.6.1 Shared Operating Environment

In an ideal situation, it is preferable to have all ballot counting performed in a strictly dedicated environment. However, if vote-counting operations are performed in an environment which is shared with other data processing functions, both hardware and software features must be present to protect the integrity of vote counting and of voting data.

The integrity of the applications software and data must be preserved by, for example, one or more of the methods described in Subsections 5.5 through 5.6. Security procedures and logging records must be used to control access to system functions.

Voting system functions must be partitioned or compartmentalized from other concurrent functions at least logically, and preferably physically as well. Procedurally

and logically, system access must be controlled by means of passwords, and restriction of account access to necessary functions only. Provisions must also be made to control the flow of information, precluding data leakage through shared system resources.

5.6.2 Interactive Queries

For equipment which operates in a central counting environment, provision must be made for external access to incomplete election returns before completion of the official count—provided that access for these purposes is authorized by the statutes and regulations of the using agency. This shall apply as well to polling place equipment that contains a removable memory module, or that may be removed in its entirety to a central place for the consolidation of polling place returns.

In this event, the system software and its security environment shall be designed so that data accessible to interactive queries shall reside in an external file, or database, that is created and maintained by the elections software under the restrictions applying to any other output report, namely, that:

- the output file or database shall have no provision for write-access back to the system; and

- persons whose only authorized access is to the file or database shall be denied write-access, both to the file or database, and to the system.

6. Quality Assurance

6.1 General

The manufacturer is responsible for designing and implementing a quality control program sufficient to ensure that the design, workmanship, and performance requirements of this standard are achieved in all delivered systems and components. This program shall, at a minimum, include procedures for specifying and procuring parts and raw materials of the requisite quality, and for their inspection, acceptance, and control. It shall require the documentation of the hardware and software development process. It shall identify and enforce all requirements for in-process inspection and testing which the manufacturer deems necessary to ensure proper fabrication and assembly of hardware; and installation and operation of software or firmware. It shall include plans and procedures for post-production environmental screening and acceptance tests. The quality control program shall also include a procedure for maintaining all data and records required to document and verify the quality inspections and tests.

Vendors who do not manufacture all components of voting systems, but who procure these components as standard commercial items for assembly and integration into voting systems, shall institute a similar quality control program to the one described, pertaining to all activities involving such components.

6.2 Responsibility for Tests

The manufacturer or vendor shall be responsible for the performance of all quality assurance tests, and for the acquisition and documentation of test data. These records shall be made available for review by the purchaser upon request.

6.3 Special Tests and Examinations

Parts and materials to be used in voting systems and components shall be selected according to their suitability for the intended application. Suitability may be determined by similarity of this application to existing standard practice, or by means of special tests. If special tests are required, they shall be designed to evaluate the part or material under conditions which accurately simulate the actual operating environment, and the resulting test data shall be maintained as part of the quality control program documentation.

6.4 Quality Conformance Inspections

The manufacturer or vendor shall inspect and test each voting system or component to verify that all inspection and test requirements of this specification have been met. A record of tests, or a certificate of satisfactory completion, shall be delivered with each system or component.

6.5 User Documentation

Complete product documentation shall be provided with voting systems or components. This documentation shall be sufficient to serve the needs of the voter, the operator, and the maintenance technician. It shall be prepared and published in accordance with standard industrial practice for electronic and mechanical equipment. It shall include, as a minimum, a Voter Manual, System Operations Manual, and System Maintenance Manual. The Voter Manual shall include a physical description of the equipment to be used by the voter, sufficient to identify and to illustrate all of its features. It shall include instructions for proper operation, and warnings to preclude improper operation of the equipment. The contents of the System Operations Manual and System Maintenance Manual are outlined in the Technical Data Package (Appendix B, Subsections B.4 and B.5, respectively).

7. Qualification Test and Measurement Procedures

7.1 Scope of Tests and Applicability Criteria

An independent test authority (ITA) shall conduct qualification tests to evaluate system compliance with the requirements of Sections 2 through 6. The examination shall encompass tests of hardware under conditions simulating the intended storage, operation, transportation, and maintenance environments; the selectively in-depth examination of software; the inspection and evaluation of system documentation; and operational tests verifying system performance and function under normal and abnormal conditions.

The scope of qualification testing should not be confused with the vendor's developmental testing. Qualification testing is the process by which a voting **system** is shown to comply with the requirements of its own design specification and with the requirements of the standards. The ITA shall evaluate the completeness of the vendor's developmental test program, including the sufficiency of vendor tests conducted to demonstrate compliance with performance specifications.

The ITA will undertake sample testing of the vendor's test modules and also design independent system-level tests to supplement and check those designed by the vendor. The ITA may utilize automated software testing tools to assist in this process if they are available for the software under examination, and if they do not duplicate vendor testing.

7.1.1 Scope of Tests

The qualification test procedure is intended to discover defects in hardware and software design and system operation which, should they occur in actual election use, could result in failure to complete election operations in a satisfactory manner.

There are three types of indicia used to assess system accuracy, reliability, and correctness. One involves the absolute logical correctness of all ballot processing software. In this case, no margin for error exists. The second revolves around operational accuracy in the recording and processing of voting data, as measured by bit error rate. Of course, it would be desirable that there be an error rate of zero. If this had to be proven by a test, however, the test itself would take an infinity of time.

The third concerns operational failure(s) or the number of unrecoverable failures in an actual time-based period of processing test ballots.

The procedure for disposition of failures or deficiencies discovered during qualification testing is described in Appendix G. This procedure recognizes that some but not necessarily all operational malfunctions (apart from software logic defects) may result in rejection. Basically, any defect that results in or may result in the loss or corruption of voting data, whether through failure of system hardware and software, through procedural deficiency, or through deficiencies in security and audit provisions, shall be cause for rejection. Otherwise, malfunctions that result from failure of either hardware or software to fully comply with other requirements of this standard will not **in every case** warrant rejection. Specific failure definition and scoring criteria are also contained in Appendix G.

7.1.1.1 Test Categories

The qualification test procedure is presented in three parts: hardware qualification tests, software qualification tests, and system-level tests. This division is somewhat artificial. In reality, there may be concurrent indications of hardware and software function, or failure to function, during certain examinations and tests. Operating tests of hardware partially exercise the software as well, and therefore, supplement software qualification. Documentation review conducted during software qualification supplements the review undertaken for system-level testing.

The qualification test procedures are presented in these three categories because test authorities frequently focus separately on hardware, software, and system-level tests. The following subsections provide information that test authorities need in each case.

Not all systems being tested are required to complete all three categories of testing. For example, if a previously-qualified system has had hardware modifications, the system may be subject only to non-operating environmental stress testing of the modified component, and a limited functional configuration audit (i.e., a partial system-level test). If a system consisting of general purpose commercial hardware or one that was previously qualified has had modifications to its software, the system is subject only to software qualification and system-level tests, not hardware testing.

7.1.1.2 Focus of Hardware Tests

Hardware testing begins with the non-operating tests (Subsection 7.3.2) that require the use of an environmental test facility. These are followed by operating tests (Subsection 7.3.3) that are performed partly in an environmental facility and partly in a standard test, laboratory or shop environment.

The non-operating tests are intended to evaluate the ability of the system hardware to withstand exposure to the various environmental conditions incidental to voting system storage, maintenance, and transportation. The procedures are based on test methods contained in Military Standard (MIL-STD) 810D, modified where appropriate, and include such tests as: transit drop, bench handling, vibration, low and high temperature, humidity, rain exposure, and sand and dust exposure. The first five tests are required. The rain, sand, and dust exposure tests are discretionary.

The operating tests involve running the system for an extended period of time under varying temperatures and voltages. This period of operation assures with confidence that the hardware meets or exceeds the minimum requirements for reliability, data reading, and processing accuracy contained in Subsections 3.2.5 and 3.2.6. The procedure emphasizes equipment operability and data accuracy; it is not an exhaustive evaluation of all system functions. Moreover, the severity of the test conditions has, in most cases, been reduced from that specified in the Military Standards to reflect commercial and industrial, rather than military and aerospace, practice.

7.1.1.3 Focus of Software Evaluation

The software qualification tests (Subsection 7.4) encompass a number of interrelated examinations. The primary objective is to examine selectively in-depth all ballot processing source code for absolute logical correctness, for its modularity and overall construction, and its adherence to the design guidelines in Appendix E. (Since these guides are not mandatory, non-adherence would not be cause for failure of qualifications except in the most egregious instances.) Part of this code examination will be focused on the assessment of potential (or actual) hidden code.

The code inspection will be followed by a series of functional tests to verify the proper performance of all system functions controlled by the software.

7.1.1.4 Focus of System-level Tests

The hardware and software qualification tests supplement a fuller evaluation of these components performed by the system-level tests (Subsection 7.5). These system-level tests focus on the hardware and software jointly, throughout the full range of system operations. They include tests of ballot-counting logic, and include the Physical Configuration Audit (PCA) and the Functional Configuration Audit (FCA). The PCA verifies that the configuration documentation and support characteristics of the system meet all requirements. The FCA is an exhaustive verification of every system function and combination of functions cited in the vendors' documentation. Through use, the FCA verifies the accuracy and completeness of the system's Operations Manual and Maintenance Manual.

7.1.1.5 Tests of Ballot Counting Accuracy

The various options of software counting logic shall be tested during the system-level Functional Configuration Audit. Generic test ballots or test entry data for DRE systems, representing particular sequences of ballot-counting events, will test the counting logic during this audit. For example, multiple test decks for variations in straight party and cross party endorsement will be created and processed by the ITA.

7.1.1.6 Sequence of Tests and Audits

There is no required sequence for performing the system qualification tests and audits. For a new system, not previously qualified, a test using the generic test ballot decks might be performed before undertaking any of the more lengthy and expensive tests or documentation review. The test agency or vendor may, however, schedule the PCA, FCA, or other tests in any convenient order, provided that the prerequisite conditions for each test have been met before it is initiated.

7.1.2 Applicability

Equipment and ballot tally processing software (exclusive of ballot layout programs) used in electronic voting systems shall be examined and tested to determine suitability for elections use. All products custom designed for election use shall be tested in accordance with the applicable procedures contained in this section. Hardware and system software with proven performance in commercial applications other than elections, however, need not be subject to **all** of the tests.[6] Compatibility of these items with the voting environment shall be determined through functional tests integrating the standard product with the remainder of the system.

Specifically, the hardware test requirements shall apply in full to all equipment used in a voting system with the exception of the following:

- commercially available models of general purpose data processing equipment that have been designed to an ANSI or IEEE standard, have a broad field history of meeting the relevant requirements of the standards and have demonstrated compatibility with the voting system, or that otherwise have demonstrated compliance with these requirements (e.g.; Documation and PDI card readers);

6/ Standard products include off the shelf hardware (e.g.; micro and mini and mainframe CPUs, card readers, printers, and CRTs) and software (e.g.; standard compilers, operating systems, and monitor programs). Generally, such products have been designed to rigorous industrial standards and have been in wide use, permitting an evaluation of their performance history.

- production models of special purpose data processing equipment that have a history of performing successfully under conditions equivalent to election use, and that have demonstrated compatibility with the voting system (e.g.; Chatsworth card readers); and

- any ancillary devices that do not perform ballot reading, data processing, or the production of an official output report, and that do not interact with these system functions (e.g.; modems used to broadcast results to the press, printers used to generate unofficial reports, or CRTs used to monitor the vote counting process).

This equipment shall be subject to functional and operating tests performed during software evaluation and system-level testing. However, it need not undergo hardware non-operating tests. If the system is composed entirely of off the shelf hardware, then the system also shall not be subject to the 48-hour environmental chamber segment of the hardware operating tests.

Software qualification is applicable to the following:

- application programs that control and carry out ballot processing, commencing with the processing of a voting image (either from physical ballots or electronically activated images) and ending with the system's access to memory for the generation of output reports;

- specialized compilers and specialized operating systems associated with ballot processing; and

- standard compilers and operating systems that have been modified for use in the vote counting process.

Normally, only ballot processing software (as distinct from ballot layout programs) shall be subjected to selectively in-depth code inspection. If the DRE system incorporates independent processing paths, each path or module shall be examined. Functional testing of all these programs during software evaluation and system-level testing shall exercise any specially tailored software off-line from the ballot counting process (e.g.; software for preparing ballots and broadcasting results).

7.1.2.1 Test Hardware and Software

The hardware submitted for qualification testing shall be equivalent, in form and function, to the actual production versions of the hardware units. Engineering or developmental prototypes are not acceptable, unless the vendor can show that the equipment to be tested is equivalent to standard production units in both performance and construction.

The software submitted for qualification shall be identical to the escrowed version.

7.1.2.2. Modifications to Qualified Systems

Software or hardware changes introduced after the system has completed qualification will necessitate further review. The ITA will determine tests necessary for requalification. For software changes, it is likely that full software qualification and system-level tests will be undertaken.

However, a modified system will be subject only to a limited qualification testing, if it can be shown that the change does not affect demonstrated compliance with these standards. The performance of essential system functions must remain in compliance, as must the overall flow of program control, and the manner in which ballots are interpreted, or voting data are processed. The change must also fall into one or more of the following classifications:

- It is made for the purpose of correcting a defect, and test documentation is provided which verifies that the installation of the altered hardware or corrected code results solely in the elimination of the defect;

- It is made solely for the purpose of providing additional audit or report generating capability, using existing audit and reporting sub-routines;

- It is made for the purpose of enabling interaction with other equipment (general purpose or approved), or with other computer programs and databases. Procedural and test documentation must be provided to verify that such interaction does not involve or adversely affect vote counting and data storage; and

- It is made for the purpose of permitting operation on a different processor, or of using additional or different peripheral devices, and does not alter the software's structure and function.

These exceptions are intended to facilitate the correction of defects, the incorporation of improvements, the enhancement of portability and flexibility, and the integration of vote-counting software with other system and elections software. The addition of a feature or function that produces any of these effects is encouraged.

No retesting is required by the addition or alteration of utility software and device handlers that only interact with vote counting software through the Input/Output channels, as originally approved.

7.2 General Requirements

7.2.1 Documentation

The test agency shall obtain the documentation necessary for the identification of the hardware and software configuration submitted for evaluation and for the development of an appropriate test plan.

The test agency shall obtain the Technical Data Package (TDP) from the vendor submitting the voting system for qualification. The TDP contains design information to the extent necessary to define the product and its method of operation. It provides vendor technical and test data which support the vendor's claims of the system's functional capabilities and performance levels. Instructions and procedures are included governing operations to be performed by elections personnel. In addition, general maintenance documentation is furnished. A detailed description of the TDP is contained in Appendix B.

The test agency shall also obtain any other documentation necessary to conduct the Physical and Functional Configuration Audits. This documentation is specified in Subsections 7.5.1.2 and 7.5.2.2.

7.2.2 Procedure

Qualification tests shall be used to determine the degree to which a system's hardware and software comply with the standards. In general, these test procedures shall:

- verify or check equipment operational status by means of manufacturer operating procedures;
- establish the test environment or the special environment required to perform the test;
- initiate and complete operating modes or conditions necessary to evaluate the specific performance characteristic under test;
- measure and record the value or range of values for the characteristic to be tested, demonstrating expected performance levels; and
- verify, as above, that the equipment is still in normal condition and status after all required measurements have been obtained.

7.2.3 Qualification Test Plan

The testing agency shall prepare a Qualification Test Plan to define all tests and procedures required to demonstrate compliance with the functional, physical, design,

and performance requirements of the standards. A recommended outline for the test plan is contained in Appendix H.

7.2.4 Test Evaluation of Performance Criteria

Test data shall be evaluated to determine compliance with the requirements in Sections 2-6 of the standards. If any malfunction or data error is detected which would be classified as a relevant failure using the criteria in Appendix G, its occurrence, and the duration of operating time preceding it, shall be recorded for inclusion in the analysis of data obtained from the test, and the test shall be interrupted.

If the malfunction is due to a defect in software, then the test shall be terminated and system returned to the vendor for correction. If the malfunction is other than a software defect, and if corrective action is taken to restore the equipment to a fully operational condition within 8 hours, then the test may be resumed at the point of suspension. If the test is suspended for an extended period of time, the testing agency shall maintain a record of the procedures which have been satisfactorily completed. When testing is resumed at a later date, repetition of the successfully completed procedures may be waived, provided that no design or manufacturing change has been made which would invalidate the earlier test results.

Any and all failures which occurred as a result of the deficiency shall be classified as purged, and test results shall be evaluated as though the failure or failures had not occurred, if:

- the vendor submits a design, manufacturing, or packaging change notice to correct a deficiency, together with test data to verify the adequacy of the change;
- the examiner of the equipment agrees that the proposed change will correct the deficiency; and
- the vendor certifies that the change will be incorporated in all existing and future production units.

If corrective action cannot be successfully taken as defined above, then the test shall be terminated, and the equipment shall be rejected.

7.2.5 Test Conditions

Qualification tests may be performed in any facility capable of supporting the test environment. Preparations for testing, arrangement of equipment, verification of equipment status, and the execution of procedures shall be witnessed by at least one

independent, qualified observer, who shall certify that all test and data acquisition requirements have been satisfied.

When a test is to be performed at "standard" or "ambient" conditions, this requirement shall refer to a nominal laboratory or office environment, with a temperature in the range of 68 to 75 degrees Fahrenheit, and prevailing atmospheric pressure and relative humidity.

Otherwise, all tests shall be performed at the required temperature and electrical supply voltage, regulated within the following tolerances:

Temperature	± 4 degrees F
Electrical supply voltage	± 2 vac

7.2.6 Test Data Requirements

A test log of the procedure shall be maintained. This log shall identify the system and equipment by model and serial number. Test environment conditions shall be noted. All operating steps, the identity and quantity of simulated ballots, annotations of output reports, the elapsed time for each procedure step, and observations of equipment performance and, in the case of non-operating hardware tests, the condition of the equipment shall be recorded.

7.2.7 Test Fixtures

The use of test fixtures or ancillary devices to facilitate qualification testing is encouraged. These fixtures and devices may include arrangements for automating the operation of voting devices and the acquisition of test data.

The use of a fixture to ensure correctness in casting ballots by hand is recommended. Such a fixture may consist of a template, with apertures in the desired location, so that selections may be made rapidly; for example, in a series of connected sweeping motions, rather than by "hunt and peck." Such a template will eliminate or greatly minimize errors in activating test ballot patterns, while reducing the amount of time required to cast a test ballot.

For systems which utilize a light source as a means of detecting voter selections, the generation of a suitable optical signal by an external device is acceptable. For systems which rely on the physical activation of a switch, a mechanical fixture with suitable motion generators is acceptable.

The use of a simulation device, and appropriate software, to speed up the process of testing and eliminate human error in casting test ballots is recommended, provided that the simulation covers all voting data detection and control paths which are used in casting an actual ballot. In the event that only partial simulation is achieved, then

an independent method and test procedure must be used to validate the proper operation of those portions of the system not tested by the simulator.

If the vendor provides a means of simulating the casting of ballots, the simulation device is subject to the same performance, reliability, and quality requirements that apply to the voting device itself.

7.2.8 Qualification Test Report

The testing agency shall prepare a qualification test report, documenting the tests and conclusions of system compliance with the requirements of the test plan and standards. A recommended outline for the test report is contained in Appendix I.

7.3 Hardware Qualification Tests

7.3.1 Preconditions

Equipment that does not meet the preconditions described in Subsection 7.1.2, shall be tested according to the following procedures. In the event that the test authority deems it necessary to deviate from requirements pertaining to the test environment, the equipment arrangement and method of operation, the specified test procedure, or the provision of test instrumentation and facilities, the deviation shall be recorded in the test log. A discussion of the reason for the deviation, and a statement of the effect of the deviation on the validity of the test procedure, shall also be provided.

7.3.2 Environmental Tests, Non-operating

7.3.2.1 General

Environmental tests of non-operating equipment are intended to simulate exposure to physical shock and vibration associated with handling and transportation by surface and air common carriers, and to temperature conditions associated with delivery and storage in an uncontrolled warehouse environment, prior to shipment to the user or during storage after delivery. The procedures and conditions of these tests correspond generally to those of MIL-STD-810D, "Environmental Test Methods and Engineering Guidelines," 19 July 1983. However, the severity of the test conditions has, in most cases, been reduced to reflect commercial and industrial, rather than military and aerospace practice.

As spelled out in the Applicability Subsection 7.1.2, systems exclusively designed with off the shelf hardware implicitly meet the requirements of the non-operating tests and are not subjected to this segment of hardware testing.

Prior to each test, the equipment shall be shown to be operational, by means of the procedure contained in Subsection 7.3.2.1.5. The equipment may then be prepared as if for actual transportation or storage, and subjected to one or more of the following procedures, as required. After each procedure has been completed, the equipment status will again be verified as in Subsection 7.3.2.1.5.

The following requirements for equipment preparation, functional tests, and inspections shall apply to each of the non-operating test procedures.

7.3.2.1.1 Pretest Data

The test technician shall verify that the equipment is capable of normal operation. Equipment identification, environmental conditions, equipment configuration, test instrumentation, operator tasks, time-of-day or test time, and test results shall be recorded.

7.3.2.1.2 Preparation for Test

The equipment shall be prepared as for shipping or storage, with any protective enclosures or internal restraints normally used for transportation and handling.

7.3.2.1.3 Mechanical Inspection and Repair

After the test has been completed, the devices shall be removed from their containers, and any internal restraints shall be removed. The exterior and interior of the devices shall be inspected for evidence of mechanical damage, failure, or dislocation of internal components. Devices shall be adjusted or repaired, if necessary.

7.3.2.1.4 Electrical Inspection and Adjustment

After completion of the mechanical inspection and repair, routine electrical maintenance and adjustment may be performed, according to the manufacturer's standard procedure.

7.3.2.1.5 Operational Status Check

When all tests, inspections, repairs, and adjustments have been completed, normal operation shall be verified by conducting an operational status check.

During this process, all equipment shall be operated in a manner and environment which simulates election use to verify the functional status of the system. Prior to the conduct of each of the environmental hardware non-operating tests, a supplemental test shall be made to determine that the operational state of the equipment is within acceptable performance limits.

The following procedures shall be followed to verify the equipment status:

Step 1 Arrange the system for normal operation.

Step 2 Turn on power, and allow the system to reach recommended operating temperature.

Step 3 Perform any servicing, and make any adjustments necessary, to achieve operational status.

Step 4 Operate the equipment in all modes, demonstrating all functions and features which would be used during election operations.

Step 5 Verify that all system functions have been correctly executed.

7.3.2.1.6 Failure Criteria

If the equipment evidences a relevant failure following any one of the non-operating test procedures, the method for disposition of failed equipment contained in Appendix H shall apply.

7.3.2.2 Transit Drop Test

7.3.2.2.1 Applicability

All systems and components regardless of type shall meet the requirements of this test. The transit drop test is intended to simulate, in a non-destructive manner, the experience (drops) of the equipment over its expected life. The classifications and number of drops are based on type of usage, not on weight per se. The tests employs the concept of a "constant potential energy formula" in which the drop height varies inversely with weight. Table 7.3.3.2-I shall be used to determine height and number of drops.

The equipment may be packaged for shipment prior to the conduct of the transit drop test.

Table 7.3.2.2.-I
Transit Drop Test

Operating Class	Number of Drops	Note
Portable	On each face, edge and corner, total of 26	A,B
Movable	Twice on each bottom edge and corner, total of 16	A,C
Fixed	On each bottom corner and edge, total of 8	A,C

Notes:

A. Potential energy at release shall be equal to 200 foot-pounds. Drop height shall be equal to (12 x 200/Weight) in inches, where Weight includes the weight of the transport container, if any. For example, if the weight of the equipment and its container is 60 pounds, then:

Weight = 60 lb.
Drop height = (12 x 200 / 60) = 40 in.

B. Drops shall be made from a quick-release hook or drop tester. The test item shall be oriented so that upon impact a line from the struck corner or edge to the center of gravity of the test item is perpendicular to the impact surface.

C. Corner drops shall be made as in Note B. Edge drops shall be made by supporting each of the two corners of one edge on blocks 8 inches in height. The opposite end of the item shall be raised to and allowed to fall freely from a height equal to the lesser of

(1) twice the height computed as in Note A, or

(2) the maximum height which can be reached without overturning the test item.

If the horizontal distance from the center of gravity of the test item to the pivot axis formed by the two supported corners is appreciably greater or less than half the distance between the pivot axis and the elevated edge, then the height to which the unsupported edge is to be raised shall be adjusted so that the product of the vertical distance travelled by the center of gravity from release to impact and the weight of the test item is maintained at 200 foot-pounds.

7.3.2.2.2 Procedure

Step 1 Install the test item in its transit or combination case as prepared for delivery.

Step 2 Perform the test, using the number of drops and drop height as specified in Table 7.3.3.2-I.

7.3.2.3 Bench Handling Test

7.3.2.3.1 Applicability

All systems and components, regardless of type, shall meet the requirements of this test. This test is equivalent to the procedure of MIL-STD-810D, Method 516.3, Procedure VI.

7.3.2.3.2 Procedure

Step 1 Place each piece of equipment on a level floor or table, as for normal operation or servicing.

Step 2 Make provision, if necessary, to restrain lateral movement of the equipment or its supports at one edge of the device. Vertical rotation about that edge shall not be restrained.

Step 3 Using that edge as a pivot, raise the opposite edge to an angle of 45 degrees, to a height of four inches above the surface, or until the point of balance has been reached, whichever occurs first.

Step 4 Release the elevated edge so that it may drop to the test surface without restraint.

Step 5 Repeat steps 3 and 4 for a total of six events.

Step 6 Repeat steps 2, 3, and 4 for the other base edges, for a total of 24 drops for each device.

7.3.2.4 Vibration Test

7.3.2.4.1 Applicability

All systems and components, regardless of type, shall meet the requirements of this test. This test is equivalent to the procedure of MIL-STD-810D, Method 514.3, Category 1—Basic Transportation, Common Carrier.

7.3.2.4.2 Procedure

Step 1 Attach instrumentation as required to measure the applied excitation.

Step 2 Mount the equipment on a vibration table with the axis of excitation along the vertical axis of the equipment.

Step 3 Apply excitation as shown in MIL-STD-810D, Method 514.3-1, "Basic transportation, common carrier, vertical axis", with low frequency excitation cutoff at 10 Hz, for a period of 30 minutes.

Step 4 Repeat steps 2 and 3 for the transverse and longitudinal axes of the equipment with the excitation profiles shown in Figures 514.3—2 and 514.3—3, respectively.

Note: The total excitation period equals 90 minutes, with 30 minutes' excitation along each axis.

7.3.2.5 Low Temperature Test

7.3.2.5.1 Applicability

All systems and components, regardless of type, shall meet the requirements of this test. This test is equivalent to the procedure of MIL-STD-810D, Method 502.2, Procedure I—Storage. The minimum temperature shall be -15 degrees F.

7.3.2.5.2 Procedure

Step 1 Arrange the equipment as for storage. Install it in the test chamber.

Step 2 Lower the internal temperature of the chamber at any convenient rate, but not so rapidly as to cause condensation in the chamber, and in any case no more rapidly than 10 degrees F per minute, until an internal temperature of -15 degrees F has been reached.

Step 3 Allow the chamber temperature to stabilize. Maintain this temperature for a period of 4 hours after stabilization.

Step 4 Allow the internal temperature of the chamber to return to standard laboratory conditions, at a rate not exceeding 10 degrees F per minute.

Step 5 Allow the internal temperature of the equipment to stabilize at laboratory conditions before removing it from the chamber.

Step 6 Remove the equipment from the chamber and from its containers, and inspect the equipment for evidence of damage.

7.3.2.6 High Temperature Test

7.3.2.6.1 Applicability

All systems and components, regardless of type, shall meet the requirements of this test. This test is equivalent to the procedure of MIL-STD-810D, Method 501.2, Procedure I—Storage. The maximum temperature shall be 150 degrees F.

7.3.2.6.2 Procedure

Step 1 Arrange the equipment as for storage. Install it in the test chamber.

Step 2 Raise the internal temperature of the chamber at any convenient rate, but in any case no more rapidly than 10 degrees F per minute, until an internal temperature of 150 degrees F has been reached.

Step 3 Allow the chamber temperature to stabilize. Maintain this temperature for a period of 4 hours after stabilization.

Step 4 Allow the internal temperature of the chamber to return to standard laboratory conditions, at a rate not exceeding 10 degrees F per minute.

Step 5 Allow the internal temperature of the equipment to stabilize at laboratory conditions before removing it from the chamber.

Step 6 Remove the equipment from the chamber and from its containers, and inspect the equipment for evidence of damage.

7.3.2.7 Humidity Test

7.3.2.7.1 Applicability

All systems and components regardless of type shall meet the requirements of this test. This test is similar to the procedure of MIL-STD-810D, Method 507.2, Procedure I—Natural Hot-Humid. It is intended to evaluate the ability of the equipment to survive exposure to an uncontrolled temperature and humidity environment during storage. This test lasts for ten days.

The equipment shall be in a non-operating, storage configuration, and a protective cover or enclosure shall be in place if one is intended to be used during storage.

7.3.2.7.2 Procedure

Step 1 Install the equipment in the test chamber. Adjust the chamber conditions to those given in MIL-STD-810D Table 507.2-I, for the time 0000 of the Hot-Humid cycle (Cycle 1).

Step 2 Perform a 24-hour cycle with the time and temperature-humidity values specified in Figure 507.2-1, Cycle 1.

Step 3 Repeat Step 2 until 5, 24-hour cycles have been completed.

Step 4 Continue with the test commencing with the conditions specified for time = 0000 hours.

Step 5 At any convenient time in the interval between time = 120 hours and time = 124 hours, place the equipment in an operational configuration, and perform a complete operational status check as defined in Subsection 7.3.2.1.5.

Step 6 If the equipment satisfactorily completes the status check, continue with the sixth 24-hour cycle.

Step 7 Perform 4 additional 24-hour cycles, terminating the test at time = 240 hours.

Step 8 Remove the equipment from the test chamber and inspect it for any evidence of damage.

7.3.2.8 Rain Exposure Test (Optional)

7.3.2.8.1 Applicability

This test is similar to the procedure of MIL-STD-810D, Method 506.2, Procedure II—Drip. This test is intended to evaluate the ability of the equipment to survive exposure to falling water from condensation, to leakage from upper surfaces, and to rain for a brief period of time incidental to transportation between a storage facility or polling place and a covered vehicle. This optional test is applicable to precinct or regional count systems that are transported.

The equipment shall be in a non-operating, transportable configuration, and a protective cover may be in place if one is intended to be used during transportation.

7.3.2.8.2 Procedure

Step 1 Install the equipment in the test facility. Provide a means of dispensing water at a rate of 7 gallons per square foot per hour, as illustrated in MIL-STD-810D, Figure 506.2-1.

Step 2 Subject the equipment to water falling from a height of approximately 3 feet for a period of 15 minutes.

Step 3 At the conclusion of the 15-minute exposure, remove the equipment from the test facility. Open or remove panels as necessary to allow the interior to be inspected.

Step 4 Inspect the test item for evidence of water intrusion.

7.3.2.9 Sand and Dust Exposure Test (Optional)

7.3.2.9.1 Applicability

This test is similar to the procedure of MIL-STD-810D, Method 510.2, Procedure I—Blowing Dust. This test is intended to evaluate the ability of the equipment to survive exposure to dust and fine sand that may penetrate into cracks, crevices, switches, display surfaces, and electromechanical parts.

The equipment shall be in a non-operating, stowed configuration, and a protective cover may be in place if one is intended to be used during storage.

7.3.2.9.2 Procedure

Step 1 Install the equipment in a test facility which meets the requirements of MIL-STD-810D, Section II-1.1.1.

Step 2 Adjust the test section temperature to 23 degrees C (73 degrees F) and the relative humidity to less than 30 percent. Maintain this relative humidity throughout the remainder of the test.

Step 3 Adjust the air velocity to 1.5 meters per second (300 feet per minute).

Step 4 Adjust the dust feed control for a dust concentration of 10.6 ± 7 grams per cubic meter (0.3 ± 0.2 grams per cubic foot).

Step 5 Maintain the conditions of Steps 2 through 4 for at least 6 hours.

Step 6 Stop the dust feed and increase the test section air temperature to 32 degrees C (90 degrees F). Maintain this condition until the internal temperature of the equipment has stabilized.

Step 7 Adjust the air velocity as in Step 3. Restart the dust feed to maintain the dust concentration as in Step 4.

Step 8 Continue the exposure for at least 6 hours.

Step 9 Turn off all chamber controls and allow the equipment to return to room temperature.

Step 10 Remove accumulated dust from the equipment by brushing, wiping or shaking, taking care to avoid introducing additional dust into the equipment. Do not remove dust by either air blast or vacuum cleaning.

Step 11 Inspect the interior of the equipment for evidence of dust intrusion and damage.

7.3.3 Environmental Tests, Operating

7.3.3.1 Applicability

This test is similar to the low temperature and high temperature tests of MIL-STD-810D, Method 502.2 and Method 501.2, with test conditions that correspond to the requirements of the performance standards. The temperature range for equipment operation shall be:

Ambient Temperature Range, degrees F	
Min	Max
40	100

In this test, the software need only operate to the extent necessary to enable the identification of hardware failures or the suspected inability of the system to perform all of the functions to be evaluated in the Functional Configuration Audit during system-level testing. Off the shelf hardware may not be subjected to the 48-hour chamber segment of the operating environmental tests.

7.3.3.2 Procedure

This procedure involves system operation under various environmental conditions for at least 163 hours. (See Appendix F for the calculation of required operating hours.) During 48 hours of this operating time, the device shall be in a test chamber. For the remaining hours, the equipment shall be operated at room temperature, outside the

chamber. The system shall be energized for the entire period of this test; the power may be disconnected only if necessary for removal of the system from the test chamber.

Operation shall consist of ballot-counting cycles which vary with system type. An output report need not be generated after each counting cycle; the interval between reports, however, should be no more than 4 hours to keep to a practical minimum the time between the occurrence of a failure or data error and its detection.

Test Ballots per Counting Cycle

Precinct count systems	100 ballots
Central count systems	300 ballots

Test ballots shall be punched, marked, or, on DRE machines, cast to produce a statistically significant number of votes. The recommended pattern of votes is one chosen to facilitate visual recognition of the reported totals; this pattern need not exercise all possible voting locations or all ballot interpretation logic features. Each ballot shall contain a minimum of 10 cast votes. System features such as data quality tests, error logging, and audit reports shall be enabled during the test.

During each 12 hour segment of the following test protocol, the equipment shall be operated for at least 12 ballot-counting cycles; it is recommended that the interval between successive cycles not exceed 2 hours. Each operating cycle shall consist of processing the number of ballots indicated in the preceding chart. The requirements of Sections 3 and 4 shall be tested, and the results recorded. The detail and quantity of those results shall be sufficient to permit the statistically meaningful determination of the level of performance achieved for each characteristic.

Step 1 Arrange the equipment in the test chamber. Connect as required and provide for power, control and data service through enclosure wall.

Step 2 Set supply voltage at 117 vac.

Step 3 Energize the equipment, and perform an operational status check as in Section 7.3.2.1.5.

Step 4 Set the chamber temperature at the low operating limit per Section 7.3.3.1, 40 degrees F observing precautions against thermal shock and condensation.

Step 5 Begin 24 hour cycle.

Step 6 At T=4 hrs, lower the supply voltage to 105 vac.

Step 7 At T=8 hrs, raise the supply voltage to 129 vac.

Step 8 At T=11:30 hrs, return supply voltage to 117 vac and return chamber temperature to lab ambient, observing precautions as in Step 4.

Step 9 At T=12:00 hrs, set the chamber temperature at the high operating limit, as in Step 4.

Step 10 Repeat Steps 5 through 8, with temperature at the high operating limit, complete at T=24 hrs.

Step 11 Set the chamber temperature at the low operating limit as in Step 4.

Step 12 Repeat the 24 hour cycle as in Steps 5-10, complete at T=48 hrs.

Step 13 After completing the second 24 hour cycle, disconnect power from the system and remove it from the chamber.

Step 14 Reconnect the system as in Step 2, and continue testing for the remaining period of operating time required as described in Appendix F until the ACCEPT/REJECT criteria of Subsection 7.3.3.4 have been met.

7.3.3.3 Data Accuracy

Accuracy shall be measured as bit error rate, the ratio of uncorrected data bit errors to the number of total data bits processed. The bit error rate shall include errors from any source during the reading, recording, and processing of votes.

There are two types of error which can affect the accuracy of vote counting. The first type consist of errors which occur randomly over time, at some average frequency. These are the errors sometimes associated with "noise." For every "plus" there will be a "minus." These "random" errors will be present in all systems to some extent, usually quite small. Testing determines the extent of these errors.

The second type of error consists of those biased in one direction or another. For example, "bias" errors in program logic could result in some or all of Candidate A's votes going to Candidate B, some of B's votes going to Candidate C, some of C's votes going to Candidate D. In hardware, "bias" errors could result in a memory location always stuck at "0" or "1", no matter what the program is trying to write in that location. Bias errors are not permissible in any system. Any such error detected during the tests shall result in the immediate rejection of the system.

7.3.3.4 Accept/Reject Criteria

Successful completion of the Operating Environmental tests shall be determined by two criteria. The first of these is measured by the number of failures as defined in Appendix G. The second is measured by the accuracy of the vote count evaluated

using the test design and procedures described in Appendix F, Subsection F.5. Subsection F.6 contains step by step protocols for resolving discrepancies during data accuracy testing.

7.4 Software Qualification Tests

Software meeting the conditions described in Section 7.1.2 shall be examined and tested according to the following procedures.

7.4.1 Review of Documentation

The test agency shall verify that the documentation submitted by the vendor is sufficient to enable source code review, and the design and conduct of all tests at any level of the software structure to verify that the software meets the vendor's design specifications and the requirements of the performance standards.

7.4.2 Source Code Review

The test agency shall compare the source code to the vendor's software design documentation to ascertain how completely the ballot counting program conforms to the vendor's specifications. Source code inspection will include an assessment of its logical correctness, the adequacy of the code's modularity and construction, the implementation of algorithms in assembly language (if used), the absence of hidden code, and the extent to which the following "industry standard" characteristics are incorporated:

- Simplicity: the straightforwardness of the design, such as avoidance of complex structures and obscure algorithms.

- Understandability: the ease with which the intent and function of the code can be ascertained and verified.

- Testability: the construction of code so as to incorporate implicit or explicit points or features to test the flow of data and control within modules and at module interfaces.

- Robustness: a property of software design that is enhanced by editing and range specification, by the incorporation of controls or traps for immediate detection of errors to prevent their propagation throughout the rest of the code and to provide a means of recovery without loss of control or data, and by data typing possible in programs using high-level language.

- Security: the inclusion of provisions to prevent unauthorized access, or to detect and control it should it be attempted.

- Usability: the ability of the system to be operated without recourse to excessive or obscure control procedures (e.g.; text messages rather than numerical error codes which require the user to consult a table).

- Installability: the ease with which a system can be made fully operational after delivery.

- Maintainability: the ease with which defects can be identified, corrected, and validated in the field.

- Modifiability: the ease with which new features can be incorporated into existing software.

Further, the code review will entail a check for the presence of desirable design characteristics noted in Appendix E. Since these guidelines are advisory, non-adherence in the strictest sense will not be cause for failing qualification testing. Egregious instances of non-compliance (e.g. spaghetti code) shall be cause for failure.

7.4.3 Functional Tests

For all systems, regardless of system type, test cases shall be designed to exercise each system function controlled by software. This includes tests for each module as well as for the program as a whole. Tests shall be performed to exercise the operating system and other programs interfacing with the ballot processing program, as well as the vote tally program itself. The test agency may review vendor test data to determine if those tests have already exercised all functions before designing further tests.

These tests shall verify proper performance of all system functions claimed in the vendor documentation, and the capabilities and features required by the Software Standards, Section 4, such as ballot interpretation logic. Ballots processed and counted during hardware operating test procedures may serve to satisfy part of software qualification, provided that the ballots were cast equivalent to procedures below.

7.4.3.1 Precinct Count System Software

As a minimum, the following procedures shall be performed during the functional tests. They need not be performed in the sequence listed, provided the necessary precondition of each procedure has been met.

- Procedures to Prepare Elections Programs
  (a) verify resident firmware, if any;
  (b) prepare software or firmware to simulate all ballot format and logic options for which the system will be used;

(c) verify program memory device content; and
(d) obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs.

- Procedures to Program Precinct Ballot Counters
  (a) install program and data memory devices, or verify presence if resident; and
  (b) verify operational status of hardware as in Subsection 7.3.2.1.5.

- Procedures to Simulate Opening of the Polls
  (a) perform procedures required to prepare hardware for election operations;
  (b) obtain "zero" printout or other evidence that data memory has been cleared;
  (c) verify audit record of pre-election operations; and
  (d) perform procedure required to open the polling place and enable ballot counting.

- Procedures to Simulate Counting Ballots
  Cast test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Subsection 4.8.4.

- Procedures to Simulate Closing of Polls
  (a) perform hardware operations required to disable ballot counting and close the polls;
  (b) obtain data reports and verify correctness; and
  (c) obtain audit log and verify correctness.

7.4.3.2 Central Count System Software

As a minimum, the following procedures shall be performed during the functional tests. They need not be performed in the sequence listed, provided the necessary preconditions of each procedure have been met.

- Procedures to Prepare Elections Programs
  (a) verify resident firmware, if any;
  (b) prepare software or firmware to simulate all ballot format and logic options for which the system will be used, and to enable simulation of counting ballots from at least 10 polling places or precincts;
  (c) verify program memory device content; and
  (d) procure test ballots with formats, voting patterns, and format identifications sufficient to verify performance of the test election programs.

- Procedures to Simulate Counting Ballots
  Count test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Subsection 4.8.4.

- Procedures to Simulate Election Reports
  (a) obtain reports at polling places or precinct level;
  (b) obtain consolidated reports, if this is a feature of the system;
  (c) provide query access, if this is a feature of the system;
  (d) verify correctness of all reports and queries; and
  (e) obtain audit log and verify correctness.

7.5 System-level Tests

System-level qualification tests are those requiring the integrated operation of both hardware and software. They include two audits: one, an audit of the physical attributes of the system; the other, the audit and testing of the functional attributes.

The system-level qualification tests shall include the tests (volume, stress, usability, security, performance, and recovery) described in Appendix H. These tests assess the system's response to a range of abnormal conditions initiated in an attempt to compromise the system. These tests may be part of the audit of the system's functional attributes, or may be conducted separately.

The total number of ballots to be processed by each precinct counting device during these tests shall be at least ten times the number of ballots expected to be counted on a single device in an election (500 to 750), but in no case less than 5,000. The number of test ballots for each central counting device shall be at least thirty times the number that would be expected to be voted on a single precinct count device, but in no case less than 15,000.

7.5.1 Physical Configuration Audit

The Physical Configuration Audit (PCA) compares the voting system components submitted for qualification to the vendor's technical documentation. The audit shall establish a configuration baseline of the software and hardware to be tested. It shall also confirm whether the vendor's documentation is sufficient for the user to install, validate, operate, and maintain the voting system. MIL-STD-1521 can be used as a guide when conducting this audit.

The test agency shall examine the vendor's source code against the submitted documentation during the PCA to verify that the software conforms to the vendor's specifications. This review shall include an inspection of all records of the vendor's release control system. If changes have been made to the baseline version, the test

agency shall verify that the vendor's engineering and test data are for the software version submitted for qualification.

If the software is to be run on any equipment other than a standard mainframe data processing system, minicomputer, or microcomputer, the PCA shall also include a review of all drawings, specifications, technical data, and test data associated with the system hardware. This examination shall establish the system hardware baseline associated with the software baseline.

To assess the adequacy of user acceptance test procedures and data, vendor documents containing this information shall be reviewed against the system's functional specifications. Any discrepancy or inadequacy in the vendor's plan or data shall be resolved prior to beginning the system-level functional and performance tests.

All subsequent changes to the baseline software configuration shall be subject to reexamination. All changes to the system hardware that may produce a change in software operation shall also be subject to reexamination.

7.5.1.1 Vendor Support

The vendor shall provide a list of all documentation and data to be audited. Vendor technical personnel shall be available to assist in the performance of the PCA.

7.5.1.2 Technical Data

The vendor shall provide the following technical data in support of the Physical Configuration Audit:

- identification of all items that are to be a part of the software release;
- specification of compiler (or choice of compilers) to be used to generate executable programs.
- identification of all hardware that interfaces with the software;
- configuration baseline data for all hardware that is unique to the system;
- copies of all software documentation intended for distribution to users, including program listings, specifications, operations manual, voter manual, and maintenance manual;
- user acceptance test procedures and acceptance criteria;
- identification of any changes between the physical configuration of the system submitted for the PCA and that submitted for the FCA, with a

certification that any differences do not degrade the functional characteristics; and

- in the event that changes are being submitted for previously-qualified software, a description of all such changes, and the results of all tests performed to verify the proper function of the changes.

7.5.2 Functional Configuration Audit

The Functional Configuration Audit (FCA) encompasses an examination of vendor tests, and the conduct of additional tests, to verify that the system hardware and software perform all the functions described in the vendor's documentation (See Appendix B). It includes a test of system operations in the sequence in which they would normally be performed. (MIL-STD-1521 may be used as a guide when conducting this audit.)

The test agency shall review the vendor's test procedures and test results to determine if the vendor's specified functional requirements have been adequately tested. This examination shall include an assessment of the adequacy of the vendor's test cases and input data to exercise all system functions, and to detect program logic and data processing errors, if such be present.

The test agency shall perform or supervise the performance of additional tests to verify nominal system performance in all operating modes, and to verify on a sampling basis the vendor's test data reports. If vendor developmental test data is incomplete, the test authority shall design and conduct all appropriate module and integrated functional tests. The FCA may be performed in the facility either of the test agency or of the vendor, and shall use and verify the accuracy and completeness of the System Operations and Maintenance Manuals.

7.5.2.1 Vendor Support

The vendor shall provide a list of all documentation and data to be audited, and vendor technical personnel shall be available to assist in the performance of the FCA.

7.5.2.2 Technical Data

The vendor shall provide the following technical data in support of the Functional Configuration Audit:

- copies of all procedures used for module or unit testing, integration testing, and system testing;

- copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests; and

- records of all tests performed by the procedures listed above, including error corrections and retests.

7.5.3 Additional Tests

Demonstration of the system's capability to permit voters to make selections and cast ballots in accordance with Subsection 3.2.4.2.6 shall be made by means of a suitable test, using persons without visual or dexterity handicaps to fully vote a fully-configured ballot, making a statistically-significant percentage of the allowable selections by means of write-in votes. In this test, each voter shall have a completed sample ballot to use as a guide.

8. Acceptance Tests

8.1 General

Acceptance tests are performed by the jurisdiction procuring the system, with or without the assistance of ITA's, state officials or outside consultants. Acceptance testing is sometimes called "validation" testing. It is a means of demonstrating that the voting system hardware and software, as delivered and installed, satisfy all of their functional requirements, and any other requirements specified in the procurement documentation, as it will operate in the user's environment.[7]

The purpose of the acceptance test is to exercise fully all, or a computed sample of, the equipment being accepted. The governing criteria for acceptance consist of the requirements of the contract or procurement documentation, none of which are addressed in this standard.

Acceptance testing requires substantial resources. System users shall prepare criteria for their acceptance test plans to validate system specifications in the most efficient and cost-effective manner. Typically, test case designs will vary with the size of the jurisdiction, the quantity and type of equipment being purchased, and the specific terms of the system procurement that must be validated. Therefore, it is not possible to design one test plan that will satisfy all of the requirements of all of the potential users of the system. However, many test requirements will be common to many states and localities, and these generally-applicable requirements are described below. They include functional tests that exercise the required operational modes of all units delivered, and performance tests that are high volume ballot processing tests conducted on all central count systems, or on a sample of the precinct count systems delivered.

As a minimum, the user shall prepare test plans, procedures and test cases to validate system performance throughout all phases of the election, beginning with ballot definition and ending with post-election cleanup and election audit. The test plans may take any form that serves the purposes of the user, and the test procedure may incorporate the following types of tests in any convenient order.

7/ To some extent, the acceptance tests will duplicate some of the functional and performance tests conducted during qualification. This is to confirm that each of the voting system units delivered conforms to the characteristics demonstrated in the qualification tests.

8.2. Typical Acceptance Test Scenario

Simulation of primary and general elections with voting systems which include ballot-counting equipment used at the polling place, shall include tests of this equipment and of its interfaces with general purpose data processing equipment used to consolidate the individual polling place returns. The tests shall validate both the polling place hardware and software.

Central counting systems may include both specialized hardware and general purpose data processing equipment. If specialized equipment is used, then the acceptance test shall validate both the hardware and software. If only general purpose equipment is used, then the acceptance test need only validate the software.

An adequate acceptance test will demonstrate each of the system's features and functions, under conditions that realistically simulate actual primary and general election operations. For P&M systems, this simulation will require the use of several decks of test ballots, punched or marked in such a way as to produce predetermined numbers of valid votes for each candidate in each simulated office, and for and against each proposition or measure. The same methodology in simulation will be used for DRE systems.

A typical scenario for P&M system acceptance testing might include the following sequence of events:

- Preliminary Procedures

  (a) prepare test plan and procedures
  (b) prepare or collect training material
  (c) define test ballot layouts
  (d) build election-specific files
  (e) prepare election firmware and software
  (f) prepare test ballots
  (g) validate election materials

- System Set-up

  (a) assemble system equipment
  (b) conduct equipment functional tests (i.e.; power on—verify ready status, check diagnostics)
  (c) verify operational status of all equipment
  (d) install test election software (central count) and firmware (precinct count)
  (e) conduct system readiness tests
  (f) verify pre-election ready status

- System Exercises

  (a) conduct L&A tests
  (b) initialize equipment (precinct count)
  (c) open polling places (precinct count)
  (d) cast test ballots
  (e) count test ballots (P&M) and obtain machine and polling place reports (all applicable systems)
  (f) close polling places (precinct count)
  (g) simulate inclusion of absentee ballots
  (h) obtain preliminary election data reports
  (i) obtain consolidated jurisdiction-wide reports, and test all operations associated with transmission of memory data to central consolidation facility (if applicable)
  (j) simulate inclusion of write-in ballots
  (k) simulate inclusion of uncounted precinct ballots
  (l) obtain official canvass of election

8.3 Test Materials

In addition to the ballot counting program and the specialized software required to interpret ballot formats for the simulated elections, one or more decks of test ballots shall be required. Test ballot formats shall provide for the demonstration of all options required or enabled by the jurisdiction.[8]

The P&M test decks used for simulating elections shall be marked so that unique totals are produced for each candidate within any office. The number of ballots to be counted in these tests will be large; however, the test decks may be reprocessed (as long as they are readable) until the desired election size has been simulated.

8.4 Test Fixtures

The use of test fixtures or ancillary devices to facilitate qualification testing is recommended. These fixtures and devices may include arrangements for automating the operation of voting devices and the acquisition of test data.

The use of a fixture for DRE systems to assure correctness in casting ballots by hand is encouraged. Such a fixture may consist of a template with apertures in the desired location so that selections may be made rapidly—for example, in a series of connected sweeping motions rather than by "hunt and peck." Such a template will eliminate or

8/ Test ballots should include both absentee ballots and ballots designed to exercise the system's logic and accuracy. For P&M systems, ballots should be run in both test mode and live mode.

greatly minimize errors in activating test ballot patterns, while reducing the amount of time required to cast a test ballot.

For systems which use a light source as a means of detecting voter selections, the generation of a suitable optical signal by an external device is acceptable. For systems which rely on the physical activation of a switch, a mechanical fixture with suitable motion generators is acceptable.

The use of a simulation device, and appropriate software, to speed up the process of testing and to eliminate human error in casting test ballots is recommended, provided that the simulation covers all voting data detection and control paths used in casting an actual ballot. In the event that only partial simulation is achieved, an independent method and test procedure must be used to validate the proper operation of the portions of the system not tested by the simulator.

If the vendor provides a means of simulating the casting of ballots, the simulation device is subject to the same performance, reliability, and quality requirements that apply to the voting device itself.

8.5 Functional Tests

Functional tests performed during acceptance testing are intended to validate that all systems and devices are capable of normal operation—that is, functional testing consists of operating condition testing undertaken on **all** units of equipment. Functional tests check all operational features and modes, including the system's ability to provide the required audit trails, perform required error recovery, and produce the necessary vote tabulation reports. As part of functional testing, various operational features and operating modes required in the purchase or lease contract are demonstrated by at least one test case for each mode.

To the extent that the system incorporates the following capabilities, test cases shall be designed to validate such operations and features as:

- building and testing all election parameter files;
- building and testing all election data processing files;
- preparing ballot layouts;
- validating polling place and ballot ID codes;
- producing election data reports at the polling place, and required consolidation reporting;
- logic and accuracy test ballot formats and data files;

- simulation and ancillary devices used to facilitate testing;
- status reporting and error detection;
- error and failure recovery procedures; and
- data integrity assurance, security, and access control provisions.

Functional tests of special purpose central count equipment shall include all of the above tests, and any others necessary to validate the ability to process ballots from more than one precinct.

Functional tests of voting system software that run on general-purpose data processing equipment shall include all tests similar to those listed above, that are necessary to validate the proper functioning of the software and its ability to control the hardware environment.

These tests shall also validate the ability of the software to detect and correctly act upon any error conditions which may result from hardware malfunctions. Detection capability may be contained in the software, the hardware, or the operating system. In any case, it shall be validated by any convenient means, up to and including the introduction of a simulated failure (e.g.: power off, disconnect a cable, etc.) in any equipment associated with ballot processing.

These tests shall exercise system operations such as those previously noted in the acceptance test scenario, and those listed in Appendix J. A reasonable number of ballots shall be processed during these tests; at least 30 for precinct count devices, and at least 3000 for central count devices.

8.6 Performance Tests

Performance tests, often conducted simultaneously with functional tests, are used to measure compliance with the numerical requirements of the standards, such as reading accuracy rates. They include sufficient volume ballot processing tests to exercise system registers; however, the number of ballots processed is normally less than for qualification testing.

These tests shall be performed on all delivered units for central count systems (i.e.; the main system and, if any, the backup system). For precinct count systems, the tests shall be performed on a sample number of the delivered units, with the sample size varying with the size of the jurisdiction (i.e.; same proportion of precinct units delivered). The total number of precinct devices to be subjected to performance tests is computed as:

$$N = 50(\log(P)),$$

where N = number of units under test,
log = logarithm to base 10 and
P = number of polling places,
greater than or equal to 100,

with the restriction that 100 percent sampling shall apply to all cases where P is less than 100.

Both precinct count and central count systems shall be tested sufficiently to demonstrate and validate the proper organization and functioning of election parameter files, election data files, and the data processing programs used with them. The requirement for these tests, and the procedures to perform them, are independent of system type and jurisdiction size.

In addition, all distributed and central data processing equipment, and all data communications equipment shall be integrated with the voting devices and absentee ballot counters in a manner representative of actual election use. All election support functions provided by this equipment shall be tested.

8.7 Ballot Reading Accuracy Tests

No physical system is capable of totally error-free performance. Eventually an error will occur, and accuracy tests are intended to validate the ability of the equipment to process large amounts of data with an error rate which is acceptably low. Errors may arise from either the hardware or the software.

Accuracy tests performed as a part of system acceptance need not be as definitive as those performed during hardware or software qualification, nor should they duplicate those tests. However, it is recommended that these tests be as rigorous as time and cost constraints permit.

A test sufficient to exercise the potentially utilized capacity of each candidate and issue register shall be performed. This test is integrated with the device and system performance test requirements specified above in Subsection 8.6.

8.8 Procedural and Input Error Tests

The user shall design test cases to validate the ability of the software to detect and correct, or indicate the occurrence of, operator procedure errors which may occur in elections use. In addition to the function and mode tests described in Subsection 8.5, the user shall also design test cases to validate the rejection of ballots with improper identification, the insertion of control cards and ballots in the wrong sequence (P&M),

or the rejection of ballot displays and removable memory devices not properly coded or programmed for the processor or the voting device in which they are to be installed (all applicable systems). These tests may be integrated with the device and system performance tests specified in Subsection 8.6.

8.9 Ballot Logic Tests

The user shall prepare a set of ballot format and logic test cases which include all instances of ballot formats and vote recording patterns authorized for use in the jurisdiction or specified in the acquisition contract. The test cases shall be designed to assign a unique number of votes to each ballot position, and to exercise features which may include, typically:

- closed and open primary elections
- partisan and non-partisan offices
- straight party voting options
- slate or group voting options
- cross-party endorsement
- presidential delegation nominations
- rotation of names within an office
- recall issues, with options
- reassembly of multi-card ballots
- split precincts
- vote for N of M
- write-in voting
- undervotes and overvotes
- totally blank ballots

8.10 Installation Tests

In the event that external libraries, programs, or files are required to support the operation of the software, the user shall design test cases to validate the correct interchange of data among all system facilities.

8.11 Procedures, Documentation, and Support

The acceptance tests shall be used to validate the user's and the vendor's procedures and documentation for elections preparation, election operations, and cleanup.

The tests shall also serve as a means for evaluating in-house and vendor personnel operations and support. The vendor shall be required to provide personnel and material support throughout the period of acceptance testing, and to correct any defect which results in failure to complete any portion of the acceptance test.

Appendix A

Applicable Documents

Appendix A

Applicable Documents

The following publications have been used for guidance in the preparation of this standard; they also contain information which is useful in interpreting and complying with the requirements of this standard.

Federal Regulations

Code of Federal Regulations, Title 47, Parts 15 and 18, Rules and Regulations of the Federal Communications Commission

Code of Federal Regulations, Title 20, Part 1910, Occupational Safety and Health Act

American National Standards

ANSI/EIA	Various standards for electronic parts and materials
ANSI/ANS 10.3-198	Guidelines for the Documentation of Digital Computer Programs, Draft, January 1985

National Institute of Standards and Technology
(formerly the National Bureau of Standards)

NIST FIPS 38	Guidelines for Documentation of Computer Programs and Automated Data Systems, National Institute of Standards and Technology, 1976
NIST FIPS 64	Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase, National Institute of Standards and Technology, 1979
NIST FIPS 99	Guideline: A Framework for the Comparison of Software Development Tools, National Institute of Standards and Technology, 1983

NIST FIPS 101	Guideline for Lifecycle Validation, Verification , and Testing of Computer Software, National Institute of Standards and Technology, 1983
NIST FIPS 105	Guideline for Software Documentation Management, National Institute of Standards and Technology, 1984
NIST FIPS 106	Guideline on Software Maintenance, National Institute of Standards and Technology, 1984

Electronic Industries Association Standards

EMCB1 - EMCB10	Electromagnetic Compatibility Bulletins
MB2, MB5, MB9	Maintainability Bulletins
QB1 - QB5	Quality Bulletins
RB5	Equipment Reliability Specification Guidelines
RB7	Accelerated Reliability Testing
RB8	Equipment Burn-in
RB9	Failure Mode and Effect Analysis
SEB1 - SEB4	Safety Engineering Bulletins
RS-232-C	Interface Between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange
RS-366-A	Interface Between Data Terminal Equipment and Automatic Calling Equipment for Data Communication
RS-404	Standard for Start-Stop Signal Quality Between Data Terminal Equipment and Non-synchronous Data Communication Equipment

Institute of Electrical and Electronics Engineers

488-1978	Standard Digital Interface for Programmable Instrumentation
696-1983	Standard 696 Interface Devices
796-1983	Standard Microcomputer System Bus

IEEE/ANSI Software Engineering Standards

729-1983	Standard Glossary of Software Engineering Terminology
730-1984	Standard for Software Quality Assurance Plans
828-1983	Standard for Software Configuration Management Plans
829-1983	Standard for Software Test Documentation
830-1984	Guide to Software Requirements Specifications
983-1986	Software Quality Assurance Planning
1008-1987	Software Unit Testing
1016-1987	Software Design Descriptions
1012-1986	Standard for Software Verification and Validation Plans

Military Standards

MIL-STD-454	Standard General Requirements for Electronic Equipment
MIL-STD-470	Maintainability Program for Systems & Equipment
MIL-STD-785	Reliability Requirements for Systems and Equipment
MIL-STD-882	Systems Safety Program Requirements
MIL-STD-975G	NASA Standard for Electronic and Electromechanical (EEE) Parts List, August, 1984

MIL-STD-1472	Human Engineering Design Criteria for Military Systems, Equipment and Facilities
MIL-STD-1521A	Technical Reviews and Audits for Systems, Equipments and Computer Programs, 1 June 1976 and Notice 2, dated 21 December 1981
DOD-STD-2167	Defense System Software Development, 4 June 1985
DOD-STD-2168	Software Quality Evaluation, 26 April 1985
DOD-STD-7935	Automated Data Systems (ADS) Documentation, 15 February 1983

Appendix B

Technical Data Package

Appendix B

Technical Data Package

B.1 Introduction

This appendix contains a description of vendor documentation relating to voting system hardware and software (including firmware) that shall be submitted with the system as a precondition of qualification testing. These items are necessary to define the product and its method of operation; to provide vendor technical and test data supporting the vendor's claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance. Other items relevant to the system evaluation shall be submitted along with this documentation (e.g.; tapes, PMDs, source and object code, and sample output report formats).

In addition to the description of items herein, required records for configuration management of hardware and software are discussed in Subsections 3.1.1 and 4.3. Quality assurance records are discussed in Section 6. Required technical data specifically necessary to conduct the Physical and Functional Configuration Audits are listed in Subsections 7.5.1.2 and 7.5.2.2.

Both formal documentation and notes of the vendor's hardware and software development process shall be submitted for qualification tests, if available and if relevant to the design and conduct of the tests. Documentation outlining this development permits assessment of the vendor's systematic efforts to test the hardware and software and correct defects. Inspection of this process also enables the design of a more precise qualification test plan. If the vendor's developmental test data is incomplete or not available, the test agency shall design and conduct the necessary tests.

At a minimum, the Technical Data Package shall contain a System Hardware Specification, a System Software Specification, a System Operations Manual, and a System Maintenance Manual.[1]

1/ Systems in existence at the time the standards are promulgated may not have all required developmental documentation. If they are subject to evaluation, vendors shall provide what information they can.

Vendors may also submit other information relevant to the evaluation of the system, such as documentation of tests performed by independent test authorities and records of the system's performance history, if any.

B.1.1 Format and Content

The recommended format and contents for items in the Technical Data Package are presented in the following sections. Other items submitted by the vendor, such as documentation of tests conducted by other test authorities, performance history, failure analysis, and corrective action may be provided in a format of the vendor's choosing.

The Technical Data Package shall include a detailed table of contents for the three primary documents, an abstract of each document and listing each of the informational sections and appendices presented within each. A summary shall be provided indicating the portions of the documents that are responsive to documentation requirements for any item presented using the vendor's format.

B.1.2 Other Uses for Documentation

Although all of this documentation is required for qualification testing, some of these same items shall also be required during the state certification process and, possibly, local level acceptance testing. This would specifically include such items as are identified in Subsections B.2.3.1, B.2.3.2, and B.2.3.4 of the System Hardware Specification; Subsections B.3.3.1, B.3.3.2, B.3.3.4, B.3.3.5.1, B.3.3.5.2, B.3.3.5.3, B.3.3.5.5, and B.3.4.3 of the System Software Specification; the System Operations Manual; and the System Maintenance Manual. It is recommended that the technical documentation required for certification and acceptance testing be deposited in escrow.

B.1.3 Protection of Proprietary Information

The vendor shall identify all documents, or portions of documents, containing proprietary information not approved for public release. Any person or test agency receiving these documents shall agree to use the information contained therein solely for the purpose of analyzing and testing the system, and shall refrain from otherwise using the proprietary information or disclosing it to any other person or agency without the prior written consent of the vendor.

B.2 System Hardware Specification

B.2.1 Scope

The vendor shall declare the scope of the specifications, thereby establishing the performance, design, test, manufacture, and acceptance requirements for the system.

B.2.2 Applicable Documents

The vendor shall list all documents controlling the design, construction, operation, and maintenance of the system. Documents shall be listed in order of precedence.

B.2.3 Requirements

The vendor shall provide descriptions of the following:

- system performance and design requirements;
- design constraints, applicable standards, and compatibility requirements;
- functional areas of the system and the interfaces between them; and
- personnel, equipment, and facility requirements for system operation, maintenance, and logistical support.

B.2.3.1 System Definition

The vendor shall delineate all operating modes and functions, and the expected values and acceptable ranges of performance attributes for each. This document shall include paragraphs that present:

- a physical description of the system and its subsystems (i.e.; environment, ballot definition, control, recording, conversion, processing, reporting, and data management);
- a theory of operation that explains each system function, and how the function is achieved in the design;
- drawings and diagrams that support the physical and functional descriptions; and
- specifications of the interfaces between subsystems and components.

B.2.3.2 System Characteristics

The vendor shall provide a detailed discussion of the characteristics of the system, including:

- Performance characteristics: basic system performance attributes and operational scenarios that describe the manner in which system functions are invoked, describe environmental capabilities, describe life expectancy, and describe any other essential aspects of system performance;

- Physical characteristics: suitability for intended use, requirements for transportation and storage, health and safety criteria, security criteria, and vulnerability to adverse environmental factors;

- Reliability: system and component reliability stated in terms of the operating functions and scenarios described in Subsection B.2.3 of this appendix, and identification of items that require special handling or operation to sustain system reliability;

- Maintainability: maintainability attributes of the system, including the Mean Time to Repair, the Maximum Time to Repair at the 95the Percentile (the maximum time required for replacement or repair of 95 percent of the failures expected to occur in a given operating period), Maintenance Rate (maintenance man-hours per operating hour), and any
mainte nance task requir ing specia l traini ng, tools, or equipm ent; and

- Environmental conditions: the ability of the system to withstand natural environments, and operational constraints on normal and test environments.

B.2.3.3 Design and Construction

The vendor shall provide sufficient data (or references to data) to identify unequivocally the system configuration submitted for qualification testing. A list of materials and components used in the system shall be included, together with the standard(s) used for their selection. Paragraphs shall be provided that describe:

- materials, processes, and parts used in the system, and the configuration control measures to ensure compliance with the system specification;

- the electromagnetic environment generated by the system, and the system's susceptibility to electromagnetic radiation present in its operating environment;

- operator and voter safety considerations, and any constraints on system operations or the use environment; and
- human engineering considerations, including provisions for access by handicapped voters.

B.2.3.4 System Support Requirements

The vendor shall describe system requirements and provisions for:

- spare parts and supplies;
- special requirements for support equipment and facilities;
- skill requirements for, and numbers of, operators and maintenance personnel;
- training requirements for election officials, operator personnel, maintenance personnel, and voters; and
- preparation for transportation and storage.

B.2.3.5 Accuracy

Accuracy requirements shall be consistent with the requirements of Section 3 of the standards. In the absence of specific numerical requirements, the vendor shall define and specify a level of accuracy that equals or exceeds the requirements for the equivalent type of system.

B.2.4 Quality Assurance Provisions

The vendor shall describe the test, inspection, and measurement procedures to be followed to ensure that the construction and installation of the system are in compliance with the system specifications defined in Subsection B.2.3 of this appendix.

B.3 System Software Specification

B.3.1 Purpose and Scope

The vendor shall summarize the function or functions that the program performs.

B.3.2 Applicable Documents

The vendor shall list all documents controlling the development of the software and its specifications. Documents shall be listed in order of precedence.

B.3.3 Requirements

The vendor shall provide the following information:

- design standards and conventions used in the development of the vendor's software;
- specifications for the environment and interfaces;
- functional specifications;
- program architecture specifications; and
- test and verification specifications.

B.3.3.1 System Overview

The vendor shall identify the system's hardware, and the environment in which the software will operate. Further, the vendor shall identify the general design, operational considerations, and constraints influencing the design of the software. The vendor shall also identify which software items were written in-house, which were procured and modified including descriptions of the modifications, and which were procured and not modified. The vendor shall include a certification that procured software items were obtained directly from the manufacturer.

B.3.3.2 Program Description

The vendor shall describe the software system concept, the specific software design objectives, the developmental methodology, and the logic structure and algorithms used to accomplish these objectives.

B.3.3.3 Standards and Conventions

The vendor shall provide information that can be used by a testing agency or state certification board as a partial basis for code analysis and test design. A description and discussion of the standards and conventions used in the preparation of the system software shall be included, as well as specifications in the development of the software.

B.3.3.3.1 Specification Standards and Conventions

The vendor shall identify all published and private standards and conventions used to document software development and testing. The vendor's internal procedures shall be provided as attachments to the software specification.

B.3.3.3.2 Programming Standards and Conventions

The vendor shall describe, or provide reference to, all standards or other documents that influenced the implementation policy, the approach, and the coding of the software. If there are exceptions to the guidelines in Appendix D, the vendor shall identify these exceptions and cite the alternate methods.

B.3.3.3.3 Test and Verification Standards

The vendor shall identify any standards or other documents that can assist in determining the program's correctness and ACCEPT/REJECT criteria.

B.3.3.3.4 Quality Assurance Standards

The vendor shall describe all standards or other documents that can be used to examine and test the software. These documents include standards for flowcharts, program documentation, test planning, and for test data acquisition and reporting.

B.3.3.4 Operating Environment

B.3.3.4.1. System Description

The vendor shall describe the system and subsystem interfaces at which inputs, outputs, and data transformations occur. This section shall describe or make reference to all operating environment factors that influence the software design.

B.3.3.4.2 Hardware Constraints

The vendor shall identify and describe the hardware characteristics that influence the design of the software, such as:

- the logic and arithmetic capability of the processor;
- memory read-write characteristics;
- external memory device characteristics;
- peripheral device interface hardware;

- data input/output device protocols; and
- operator controls, indicators, and displays.

B.3.3.4.3 Software Environment

The vendor shall identify the compiler or assembler used in the generation of executable code, and describe the operating system or system monitor. An overview of the compile-time interaction of the voting system software with library calls and linking shall also be included.

B.3.3.4.4. Interface Characteristics

The vendor shall describe the interfaces between executable code, system input/output, and control hardware.

B.3.3.5 Software Functional Specification

B.3.3.5.1. Overview

For each software mode or modes of operation, the vendor shall provide a description of the overall functions that the software performs. The functional specification defines the manner in which the software performs its intended functions. It defines program correctness and therefore serves as a basis for qualification, state certification, and acceptance testing.

The vendor shall also describe the software's capabilities or methods for detecting or handling: exception conditions, system failure, data input/output errors, error logging, for audit record generation, production of statistical ballot data, data quality assessment, and security monitoring and control.

B.3.3.5.2 Configurations and Operating Modes

The vendor shall describe the various software configurations and operating modes of the system, such as preparation for opening the polling place, recording votes and/or counting ballots, closing the polling place, and generating reports. For each software function or operating mode, a vendor shall provide: a definition of the inputs to the function or mode (with characteristics, tolerances or acceptable ranges, as applicable), an explanation of how the inputs are processed, and a definition of the outputs produced (again, with characteristics, tolerances, or acceptable ranges as applicable).

B.3.3.5.3 External Files

A definition of the information content and record formats shall be provided for any external files used for data input or output. The vendor shall also describe the procedures for file maintenance, management of access privileges, and security.

B.3.3.5.4 Security

Operating procedures for maintaining the security of the software shall be defined and identified for each system function and operating mode. This documentation shall be prepared such that these requirements can be integrated by the user into local administrative and operating procedures.

B.3.3.6 Programming Specifications

The vendor shall provide in this section an overview of the software design, its structure, and implementation algorithms. This overview shall include such items as flowcharts, HIPOs, dataflow diagrams, and other graphical techniques which facilitate understanding of the software. This section shall be prepared to facilitate understanding of the internal functioning of the individual software modules. Implementation of the functions shall be described in terms of the software architecture, algorithms, and data structures; all procedures or procedure interfaces vulnerable to degradation in data quality or security penetration shall be identified.

B.3.4 Test and Verification Specifications

B.3.4.1 Development Test Specifications

The vendor shall describe the procedures used during software development to verify logic correctness, data quality, and security. This description shall include existing standard test procedures, special purpose test procedures, test criteria, experimental design, and validation criteria. In the event that this test data is not available, the test agency shall design test cases and procedures equivalent to those ordinarily used during product verification.

B.3.4.2 Qualification Test Specifications

The vendor shall provide specifications for verification and validation of overall software performance. These specifications shall cover control and data input/output, acceptance criteria, processing accuracy, data quality assessment and maintenance, ballot interpretation logic, exception handling, security, and production of audit trails and statistical data. The specifications shall identify procedures for assessing and demonstrating the general suitability of the software for elections use. The vendor's

specifications and procedures shall be used to establish the requirements of the tests described in Section 7 of the standards.

B.3.4.3 Acceptance Test Specifications

The vendor shall provide specifications for validation of installation, acceptance, and readiness. These specifications shall define specific procedures for assessing and demonstrating the capability of the software to accommodate actual ballot formats and format logic, and for assessing and demonstrating the pre-election logic, accuracy, and security test requirements of using jurisdictions. These specifications will provide guidance to the procuring agency in developing its acceptance test plan and procedure according to the agency's contract provisions, and the election laws of the state.

B.3.5 Appendices

The vendor may provide descriptive material and data supplementing the various sections of the body of the Software Specifications. The content and arrangement of appendices shall be at the discretion of the vendor. Topics recommended for amplification or treatment in appendix form include:

- **Glossary**: A listing and brief definition of all software module names and variable names, with reference to their locations in the software structure. Abbreviations, acronyms, and terms should be included, if they are either uncommon in data processing and software development or are used in an unorthodox semantic;

- **References**: A list of references to all related vendor documents, data, standards, and technical sources used in software development and testing;

- **Program Analysis**: The results of software configuration analysis, algorithm analysis and selection, timing studies, and hardware interface studies that are reflected in the final software design and coding; and

- **Security Analysis**: A detailed description of the penetration analysis undertaken to preclude intrusion by unauthorized persons and fraudulent manipulation of elections data. Security measures, and those audit capabilities used to detect breaches in security should be included. This Appendix shall not routinely be released to the user jurisdiction programming elections.

B.4 System Operations Manual

The System Operations Manual shall provide all information necessary for system use by polling place or central counting place personnel, as applicable. The nature of the

instructions for operating personnel will depend upon whether the system is used with equipment installed in polling places, or with equipment used in a central counting environment.

The System Operations Manual shall contain all information that is required for the preparation of detailed operating procedures, and for operator training, including the sections listed below:

B.4.1 Introduction

The vendor shall provide a summary of system operating functions and modes, in sufficient detail to permit understanding of the system's capabilities and constraints. The roles of operating personnel shall be identified and related to the operating modes of the system. Decision criteria and conditional operator functions (such as error and failure recovery actions) shall be described.

The vendor shall also list all reference and supporting documents pertaining to the use of the system during elections operations.

B.4.2 Operational Environment

The vendor shall describe the system environment, and the interface between the user or operator and the system. Emphasis shall be given to the flow of functions and to the choices presented to the user or operator.

B.4.3 Operational Features

The vendor shall provide a detailed description of all input, output, control, and display features accessible to the operator or voter. The description shall include examples of simulated interactions in order to facilitate understanding of the system and its capabilities. This description shall include sample data formats and output reports, and shall illustrate and describe all status indicators and information messages.

B.4.4 Operating Procedures

The vendor shall identify and describe operating procedures required to initiate, control, and verify proper system operation. Emphasis shall be placed on operator assessment of the correct flow of system functions (as evidenced by system-generated status and information messages), and upon operator intervention required to recover from an abnormal system state. If operator intervention is required to load, initialize, and start the system, appropriate procedures and operator responses to system prompts shall be defined and illustrated.

The procedures required to enable and control the external interface to the system operating environment shall be defined and illustrated if supporting hardware and software are involved. Such information shall be provided for the interaction of the system with other data processing systems or data interchange protocols as well.

Administrative procedures and off-line operator duties (if any) shall be included if they relate to the initiation or termination of system operations, to the assessment of system status, or to the development of an audit trail.

B.4.5 Operations Support

The vendor shall define the procedures required to support system acquisition, installation, and readiness testing. These procedures may be provided by reference, if they are contained either in the System Hardware Specifications, or in other vendor documentation provided to the test agency and to system users.

The vendor shall also describe procedures for providing technical support, system maintenance and correction of defects, and for incorporating hardware upgrades and new software releases.

B.4.6 Appendices

The vendor may provide descriptive material and data supplementing the various sections of the body of the System Operations Manual. The content and arrangement of appendices shall be at the discretion of the vendor. Topics recommended for discussion include:

- **Glossary**: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer operations;
- **References**: A list of references to all vendor documents and to other sources related to operation of the system; and
- **Detailed Examples**: Detailed scenarios that outline correct system responses to every conceivable faulty operator input. Alternative procedures may be specified depending on the system state.
- **Manufacturer's Recommended Security Procedures**: This appendix shall contain all security procedures that are to be executed by the system operator.

B.5 System Maintenance Manual

The System Maintenance Manual shall provide information in sufficient detail to support election workers, data personnel, or maintenance personnel in the adjustment or removal and replacement of components or modules in the field. Technical documentation needed solely to support the repair of defective components or modules ordinarily done by the manufacturer or software developer is **not** required.

Recommended service actions to correct malfunctions or problems shall be discussed, along with: personnel and expertise required to repair and maintain the system; and equipment, materials, and facilities needed for proper maintenance. This manual shall include the sections listed below.

B.5.1 Introduction

The vendor shall describe the structure and function of the equipment (and related software) for election preparation, programming, vote recording, tabulation and reporting; in sufficient detail to provide an overview of the system for maintenance, and for identification of faulty hardware or software.

The description shall include a theory of operation that fully describes such items as:

- the electrical and mechanical functions of the equipment;
- how the processes of ballot handling and reading are performed (P&M systems);
- how vote selection and casting of the ballot are performed (DRE systems);
- how data are handled in the processor and memory units;
- how data output is initiated and controlled;
- how power is converted or conditioned; and
- how test and diagnostic information is acquired and used.

B.5.2 Maintenance Procedures

B.5.2.1 Preventive Maintenance Procedures

The vendor shall describe all required and recommended preventive maintenance tasks. The number and skill levels of personnel shall be identified. The parts, supplies, special maintenance equipment, or other resources needed for this function shall also be identified. Any maintenance tasks that must be coordinated with the

vendor or a third party shall be specified, such as coordination that may be needed for off-the-shelf items used in the system.

B.5.2.2 Corrective Maintenance Procedures

The vendor shall prepare fault detection, fault isolation, correction procedures, and logic diagrams for all operational abnormalities identified by design analysis and operating experience.

The vendor shall identify specific procedures to be used in diagnosing and correcting problems in the system hardware (or user-controlled software). Descriptions shall include steps to replace failed or deficient equipment and to correct deficiencies or faulty operations in software. The descriptions shall also note the modifications that are necessary to coordinate any modified or upgraded software with other software modules.

The vendor shall specify the number and skill levels of personnel needed to accomplish the task, together with the special maintenance equipment, parts, supplies, or other resources needed. Any coordination required with the vendor, or other party for off the shelf items, shall be indicated.

B.5.3 Testing

The vendor shall specify diagnostic tests that may be employed to identify problems in the system. In addition, tests to verify the correction of maintenance problems shall also be described.

B.5.4 Personnel and Training

B.5.4.1 Personnel

The vendor shall specify the number of personnel and skill level required to perform each of the following functions:

- preventive maintenance tasks;
- diagnosis of faulty hardware or software;
- corrective maintenance tasks; and
- testing to verify the correction of problems.

A description shall be presented of which functions may be carried out by user personnel, and those that must be performed by vendor personnel.

B.5.4.2 Training

The vendor shall specify requirements for the orientation and training of at least three levels of maintenance support personnel:

- poll workers;
- user maintenance technicians and data personnel; and
- vendor personnel.

B.5.5 Maintenance Equipment

The vendor shall identify and describe any special purpose tests or maintenance equipment recommended for fault isolation and diagnostic purposes.

B.5.6 Parts and Materials

The vendor shall provide a complete list of parts and materials; this list must contain sufficient descriptive information to identify all parts by type, size, value or range, manufacturer's designation, individual quantities needed, and the sources from which they may be obtained.

B.5.7 Facilities

The vendor shall identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance.

B.5.8 Appendices

The vendor may provide descriptive material and data supplementing the various sections of the body of the System Maintenance Manual. The content and arrangement of appendices shall be at the discretion of the vendor. Topics recommended for amplification or treatment in appendix form include:

- **Glossary**: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer maintenance;
- **References**: A list of references to all vendor documents and other sources related to maintenance of the system; and
- **Detailed Examples**: Detailed scenarios that outline correct system responses to every conceivable faulty operator input. Alternative procedures may be specified depending on the system state.

- **Maintenance and Security Procedures**: This appendix shall contain technical illustrations and schematic representations of electronic circuits, with indications of all test and adjustment points, and the nominal value and tolerance or waveform to be measured.

Appendix C

Retention of Data From Electronic Voting Systems

Appendix C

Retention of Data From Electronic Voting Systems

C.1 Background[1]

The relatively brief document retention periods imposed by state laws are not usually long enough to assure that necessary voting records will be preserved until more subtle forms of federal civil rights abuses and election crimes have been detected. It normally takes longer than 60 days for evidence to surface that fraudulent voting practices took place in connection with a given election, or that federally secured voting rights were not sufficiently protected. Accordingly, in 1960 the Congress passed a series of statutes to assure that voting documentation is preserved for a sufficient period of time to permit the federal government to discharge its limited but important responsibilities in the election area. These laws are presently codified at Title 42, United States Code, Sections 1974 through 1974e, inclusive.

Section 1974 states that election administrators are required to preserve **for 22 months** "all records and paper which came into (their) possession relating to an application, registration, payment of poll tax, or other act requisite to voting."

This retention requirement applies only to those elections where candidates for federal offices (e.g., Member of Congress, United States Senator, and/or Presidential Elector) were voted upon. It does not apply to local or state elections, unless those elections take place simultaneously with balloting for federal offices.

C.2 General Retention Requirements

Since the purpose of this law is to assist the federal government in discharging its law enforcement responsibilities in connection with civil rights and election crimes, its scope must be interpreted in keeping with that objective. As such, all documentation that may be relevant to the detection and prosecution of federal civil rights or election crimes are required to be maintained intact for the 22-month federal retention period,

---

1/ The following text in Subsections 1.0 and 2.0 are abstracted from an article appearing in the FEC Clearinghouse Journal, by Craig Donsanto, Director of Election Crimes Branch, U.S. Dept. of Justice, Vol. 12, Summer, 1985.

as long as it was generated in connection with an election which was held in whole or part to select federal candidates.

Specifically, the Department of Justice considers this law to cover:

- all voting registration records;
- all poll lists and similar documents reflecting the identity of voters casting ballots at the polls;
- all applications for absentee ballots;
- all envelopes in which absentee ballots are returned for tabulation;
- all documents containing oaths of voters;
- all documents relating to challenges to voters or to absentee ballots;
- all tally sheets and canvass reports;
- all records reflecting the appointment of persons entitled to act as poll officials or poll watchers; and
- all computer programs utilized to tabulate votes electronically.

In addition, it is the Department of Justice's view that the phrase "other acts requisite to voting" as it is used in Section 1974 requires the retention of the **ballots themselves**, at least in those jurisdictions where a voter's electoral preference is manifested by marking a piece of paper or punching holes in a computer card.

C.3 Specific Vendor Responsibilities

The list of documentation contained above in Subsection C.2 covers general items to be retained for a 22-month period, regardless of type of electronic voting used in the jurisdiction. Due to varying system design characteristics, it is not feasible to list all possible formats of database and report information that each system is or might be capable of generating.

Accordingly, it shall be the responsibility of each voting system vendor to submit to the Federal Election Commission a written request for information regarding the types and respective formats of election specific database, audit and vote data that must be retained by the user jurisdictions. The Commission, in turn, will request a formal ruling from the Election Crimes Branch of the Department of Justice. For each system, the vendor shall present detailed operational characteristics, such that DOJ can rule on specific data and document items and their preferable media (manual

and/or electronic format) that are to be retained for the auditability and reconstruction of the election process.

Subject to final definitive DOJ rulings which take into account system specific capabilities, the following section may be used as a guide in defining the types and media form of data to be retained.

C.4 General Rules for Retention of Data

The purpose in retaining an election audit trail is to leave a documented, clear record of all election activity. This requirement would applies to two time periods: the 6 month time-frame for recounts and contested elections; and the 22-month document retention. The Functional Specification and Hardware Requirements sections note performance specifications for memory, audit data, and cartridge device (PROM) integrity. This integrity figure is a technical one, established at a minimum of 6 months. It pertains to the inherent capability of such hardware to retain and secure data. A 6 month requirement is of sufficient longevity to assure that any recounts and contested elections that may extend even longer will provide all pertinent electronic data for reconstruction.

Essentially, the quantity and type of both manual and electronic data required for recounts (and subsequent contested elections) is greater than that required to be retained for the full 22-month period. All electronic data, including memory data in DRE machines, is needed for recounts. For detection and prosecution of election crimes, records other than electronic data can be successfully used (i.e.; paper or disk records of election specific data, ballot faces or Votomatic pages, printed results of the vote tally, and manual audit record data).[2]

For 22-month document retention, the general rule is that all hard-copy records produced by the election database and ballot processing systems shall be so labelled and archived. Regardless of system type, all audit trail information spelled out in Subsection 4.8 of the Standards shall be retained in its original format, whether that be real-time logs generated by the system, or manual logs maintained by election personnel. The election audit trail includes not only in-process logs of election-night (and subsequent processing of absentee or provisional ballots), but also time logs of baseline ballot definition formats, and system readiness and testing results.

At a minimum, the records shall include copies of operating procedures established for machine preparation and operation data extraction, actual ballot displays and associated records. Other information that shall be retained includes:

2/ Should potential federal prosecution become evident following election day, the Department of Justice might well petition the courts to have all electronic media and voting devices impounded.

- Results of pre-election day tests;
- All election specific database information, listings;
- Samples of test, facsimile, or machine ballots, linked to each precinct;
- All election processing reports, summaries, and results tapes;
- For DRE machines, records of individual ballot images;
- Printed list of zero totals for precinct count devices (or memory registers in central count systems);
- All audit record data, logs, status reports, tapes, and disks; and
- All security records and listings (and violations thereof).

In many voting systems, the source of election specific data (and ballot formats) is contained in a database file. In precinct count systems, this data is used to program cartridges for each machine, establish ballot layout, and generate tallying files. The preliminary thinking is that it is not necessary to retain this information on electronic cartridges if there is documented producible hard copy of all final database information. It is recommended, however, that disk storage of the aggregate summary data for each device be retained in addition to hard-copy records so that reconstruction of an election is possible without data re-entry. The same requirement and recommendation shall apply to vote results generated by each precinct device or system.

Appendix D

Hardware Design Recommendations

Appendix D

Hardware Design Recommendations

D.1 Introduction

This Appendix contains guidelines and recommended practices for the design and construction of P&M and DRE voting systems. It is intended to assist manufacturers and vendors in achieving levels of performance and quality consistent with the requirements of the standards.

Because superior electrical and mechanical performance cannot be measured at a single instant in time, the history of performance is the true measure of product quality, and this history is determined by many equipment attributes. These guidelines contain material which focuses on methods and procedures to assist voting system designers and manufacturers in assuring that performance is sustained throughout the entire life cycle of the system.

Reference is made in this document to various commercial and military standards, containing information which can be adapted to voting systems hardware. Many current designs for commercial and industrial equipment embody the principles and practices of these standards, modified where necessary to satisfy the requirements of their marketplaces. Manufacturers find that the added production costs associated with careful attention to design, parts selection, manufacturing methods, and workmanship are more than offset by reduced warranty costs. Users find that the increase in system acquisition cost is relatively minor, but the reduction in operating and support costs is quite significant.

A list of applicable federal standards is contained in Appendix A. Several aspects of design and production are covered by both commercial and military standards. In general, the military standards are broader in scope than their commercial counterparts. For this reason, they have been used for specific reference in the following sections.

The application of these guidelines to voting systems is optional. Manufacturers are encouraged to find cost-effective means for adopting them.

D.2 Reliability Analysis

The methods shown in MIL-STD-785, "Reliability Program for Systems and Equipment Development and Production," may be used to evaluate the reliability characteristics of new designs, for which test and operational data are not yet available. Reliability analysis is not complex, and it is merely the formalization of methods which all successful designers employ to "cover all the bases." The analysis begins with a definition, in numerical terms, of the functional goals or requirements which form a part of the design objective. Every design analysis task has implications of reliability, from the evaluation of design concepts, through the selection of individual parts that make up the system. One level of analysis is complete when a detailed review of the production design has been accomplished. The entire analysis is complete only when field performance has been analyzed to demonstrate that the design goals have been achieved.

The tasks listed below, taken from a military reliability standard, are typical of the activities which should be applied to the design, manufacturing, and test of commercial products, and which will produce benefits far in excess of their cost. The reliability standard cited is intended for use by military agencies which initiate system procurement programs. It directs these agencies in tailoring a general requirement to the specific needs of the program. In the same sense, the document can serve the needs of commercial system development, by forcing the recognition of activities which are crucial to the achievement of product effectiveness, and by selecting an appropriate subset of the standard tasks to accomplish them.

Reliability Analysis Tasks
Reference MIL-STD-785

Task 103: Program Reviews
Establish a requirement for reporting on progress and status at critical milestones during design, development, and production.

Task 104: Failure Reporting, Analysis, and Corrective Action
Establish a procedure for recording and analyzing failures, and for developing corrective action, if required.

Task 201: Reliability Modeling
Formulate a method for establishing and allocating design goals.

Task 203: Reliability Predictions
Determine if the design is inherently capable of meeting the reliability goal.

Task 204: Failure Modes, Effects, and Criticality Analysis
Evaluate the design. Identify the functional effects of failure, and the resulting maintenance requirements.

Task 301: Environmental Stress Screening
Develop and conduct test procedures to eliminate hazards of, and workmanship defects in, components and subassemblies prior to final assembly.

Task 304: Production Reliability Acceptance Testing
Develop and conduct test procedures to validate functional capability of systems prior to delivery.

D.3 Maintainability Analysis

Every voting system vendor is aware of the cost and effort required to support equipment in the field. Much of this cost and effort can be eliminated by careful attention to design and assembly methods which facilitate the performance of preventive and corrective maintenance tasks. This is truly an aspect of design in which the "ounce of prevention is worth the pound of cure." Performed in conjunction with the reliability analysis, which produces an estimate of the nature and frequency of maintenance requirements, the maintainability analysis can highlight requirements for test, measurement, and diagnostic capability or positive indication of failure, ease of access to internal components and circuitry, modularity of subassemblies, and the optimization of repair/replace strategy.

The following tasks of MIL-STD-470, "Maintainability Program for Systems and Equipment," are applicable to the design of voting systems.

Maintainability Analysis Tasks
Reference MIL-STD-470

Task 104: Data Collection, Analysis and Corrective Action System
Establish a method for reporting, analyzing, and correcting maintainability problems.

Task 203: Maintainability Predictions
Identify and eliminate potential maintainability problems during the design process.

Task 204: Failure Modes and Effects Analysis
Identify significant maintenance tasks and frequencies of such tasks.

Task 205: Maintainability Analysis
Develop maintenance environment and resources required for life-cycle support.

Task 206: Maintainability Design Criteria
Establish standard design practices to achieve maintainability goals.

D.4 Workmanship

The inherent quality of a design is often degraded by the selection of parts and materials which are not suited to the application, and by poor workmanship in construction and assembly. MIL-STD-454, "Standard General Requirements for Electronic Systems," is a compendium of specifications and standards covering design practice, parts and materials, and workmanship. The workmanship requirements of this standard cover both general and specific subjects. The following requirements are recommended for adoption as standard practice by manufacturers of voting systems and components.

Workmanship Requirements
Reference MIL-STD-454

Reqt. 5 - Soldering
Reqt. 7 - Interchangeability
Reqt. 8 - Electrical Overload Protection
Reqt. 9 - Workmanship
Reqt. 69 - Internal Wiring Practices

D.5 Safety

Defects in design and construction, which can result in personal injury or equipment damage, must be detected and corrected before voting systems and components are placed into service. Manufacturers, and agencies which procure and use this equipment, must adopt appropriate methods to preclude the exposure of voters and operating personnel to any hazard attendant upon its use. This exposure, and the litigation which may follow, can be avoided or ameliorated by proper attention to design, and by documenting the steps taken to eliminate or to reduce the severity of potential safety hazards.

The safety program should be formalized to the extent necessary to document the exercise of sound engineering and management judgement in avoiding all foreseeable hazards. MIL-STD-882, "System Safety Program Requirements," contains several tasks which are suitable for application to commercial equipment. The following are applicable to all voting systems. Vendors are encouraged to review the remaining tasks in this standard, and to apply them to the extent that they may be relevant to specific designs.

Safety Analysis Tasks
Reference MIL-STD-882

Task 101: System Safety Plan
Describe the tasks and activities which will identify, evaluate, and eliminate potential safety hazards.

Task 203: Subsystem Hazard Analysis
Identify hazards associated with the designs of subsystems, the interactions among them, and their operator interfaces.

Task 205: Operating and Support Hazard Analysis
Identify all hazards from any source, including software and human error, associated with system operation and maintenance.

D.6 Human Engineering

The interface between voting system equipment and the voter, the operator, and the maintenance technician, can be simplified by following the recommended practices of MIL-STD-1472, "Human Engineering Design Criteria for Military Systems, Equipment and Facilities." This document covers visual and audio displays, controls, labeling, anthropometry, and other factors that are as applicable to commercial equipment as they are to military systems.

Most design standards do not include requirements for handicapped persons. Therefore, designers of voting systems are encouraged to extend the criteria of MIL-STD-1472, and accommodate their designs to the special requirements of users and operators whose sight, hearing, speech, or mobility may be impaired, in conformity with the spirit of the Voting Accessibility for the Elderly and Handicapped Act of 1984 (Public Law 98-435).

Appendix E

Software Design Recommendations

Appendix E

Software Design Recommendations

E.1 Introduction

This Appendix is intended to familiarize voting system software users and vendors with recognized software design and coding practices. These recommended development practices should help insure that voting system software is reliable, testable, robust, and maintainable.

The specific requirements for modular software design, software documentation, and vendor developmental testing are addressed in the main body of the standards. The documents listed in Appendix A, widely used in both the commercial and military software programs, may be used as additional guidance. Their selective application to voting system software will be both beneficial and cost-effective.

E.2 Approaches to Software Design and Development

There is no single "best" way to design software. There are many programming languages for which "modern programming practices" are applicable, such as the use of program and data structures, data typing, naming conventions. There are other programming languages to which such practices are not easily applied.

Some of the following guidelines for software development are predicated upon the use of those programming languages that support structured design, such as control logic and data structures, clocking alternatives, interface protocols, shells, layered applications, security of programs and data, and no use of GOTOs or unconditional branching.

These advisory recommendations are intended to guide the design of software written in any of the programming languages commonly used for mini-computer and microprocessor systems. They are not intended to preclude the use of other languages and environments, such as those that exhibit "declarative" structure, "object-oriented" languages, "functional" programming languages, or any other combination of language and implementation that provides appropriate levels of performance, testability, reliability, and security.

E.2.1 Program Language

It is preferable to use high level programming language for that segment of the ballot tabulation software associated with the logical and numerical operations on vote data. Such languages include, but are not limited to: Pascal, COBOL, Fortran, and C.

The preferential use of high level language for logical operations does not preclude the use of assembly language for hardware-related segments, such as device controllers and handler programs. Also, operating system software may be designed in assembly language.

E.2.2 Modularity

The code for each module shall perform a single function and shall not be self-modifying; external modification of code during execution shall be prohibited.

Each unit should be uniquely named. It should follow a standard format consisting of prologue, declarative statements, and executable statements or comments, in that order.

Each unit shall have a single entry point, and a single exit point, for normal program flow. In the event of an abnormal exit induced by an error, the error condition shall be handled as close to the point of detection as possible.

No more than 50% of all modules should exceed 60 lines in length, no more than 5% of all modules should exceed 120 lines in length, and no modules should exceed 240 lines in length. The vendor should justify, in comments in the code, each module larger than 120 lines. Any unconditional branching shall be explained by detailed comments in the code.

E.2.3 Control Constructs

Voting system software should utilize any or all of the following control constructs, which are illustrated in Figures E.1 through E.5.

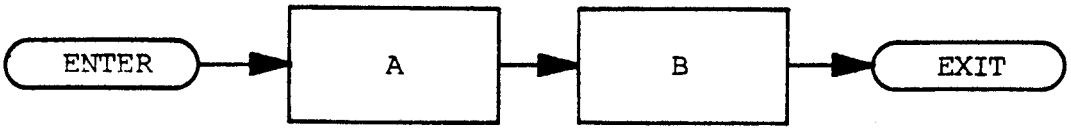
Fig. E.1	Sequence	Fig. E.4	Do - Until
Fig. E.2	If - Then - Else	Fig. E.5	Case
Fig. E.3	Do - While		

As an alternative to the Do-While and Do-Until constructs, the Loop construct shown in Figure E.6 may be used.

If the language does not contain these control constructs, the vendor should use suitable assembly language constructs, or these constructs should be simulated by code that follows their logic. If these constructs are simulated, the name form of

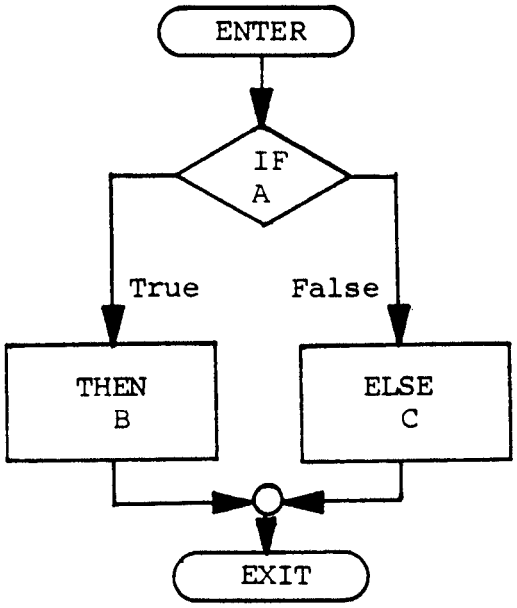
simulation should be used throughout the code. No other constructs should be used to control the logic of program execution.

The redirection of control by means of operator intervention or data-driven logic should not be allowed during the execution of any program unit. The redirection of control resulting from the calling of subroutines, procedures and functions, or by the action of exception handlers and interrupt service routines, is allowed.



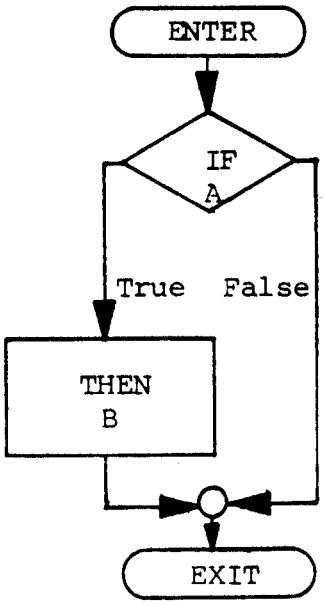
Control flows from Process A to the next in sequence, Process B.

Figure 1. SEQUENCE Construct



Basic

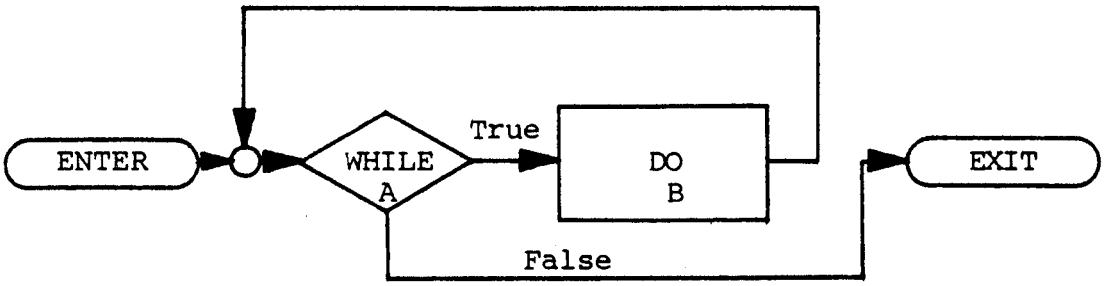
Flow of control will return to common point after executing Process B or C. A predicates the conditional execution.



Option

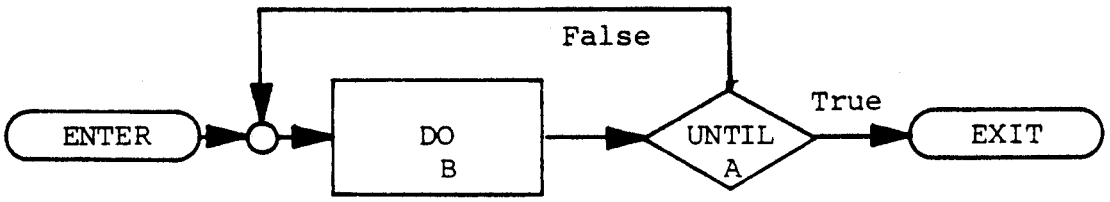
Flow of control will skip a process pending the condition of A.

Figure 2. IF-THEN-ELSE Construct



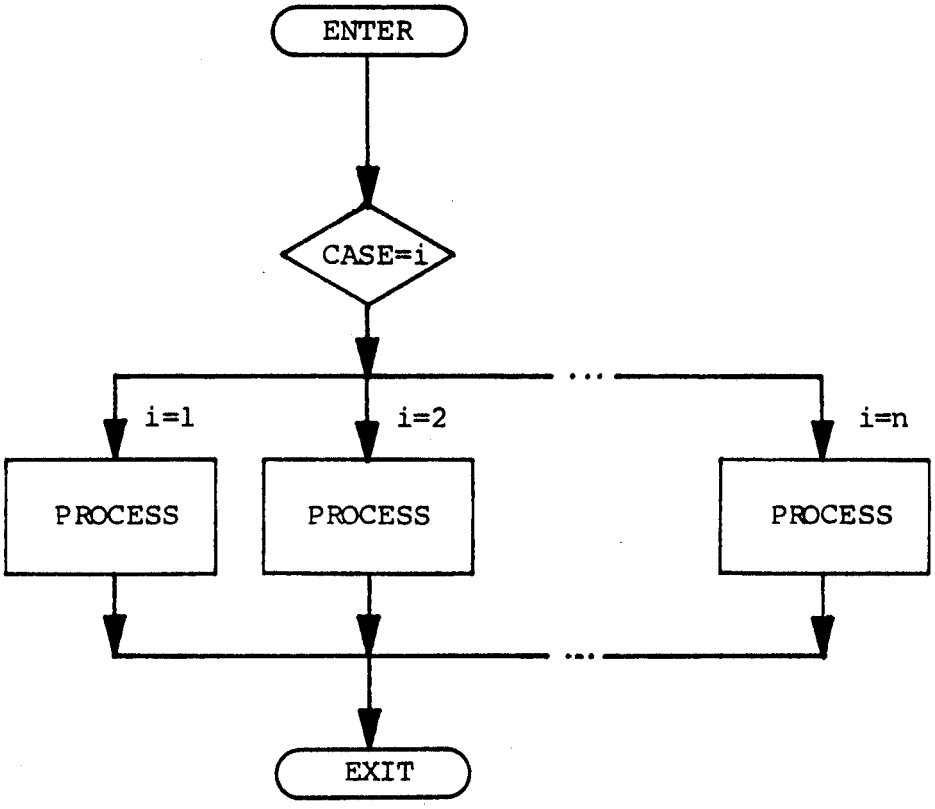
Condition A is evaluated. If found to be true, then control is passed to Process B and condition A is reevaluated. If condition A is found to be false, then control is passed out of the loop.

Figure 3. DO-WHILE Construct



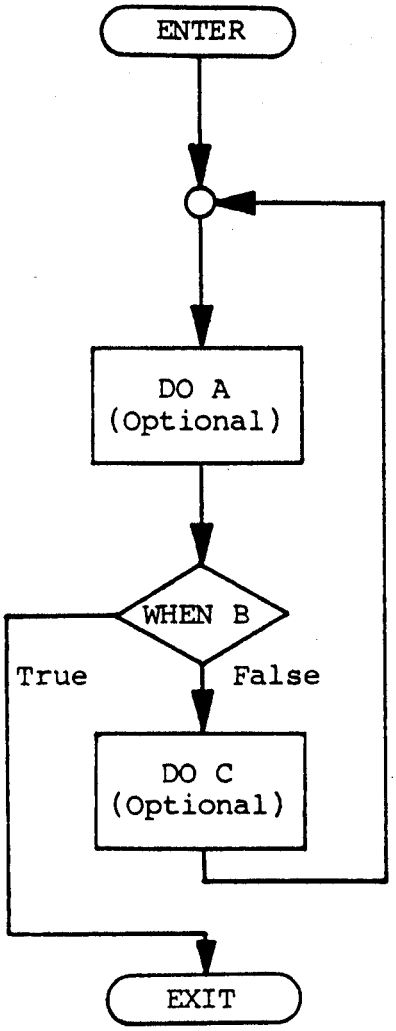
Similar to DO-WHILE, excet that the test of condition A is performed after Process B has executed. If condition A is true, control is passed out of the loop.

Figure 4. DO-UNTIL Construct



Control is passed to a Process based on the value of i.

Figure 5. CASE Construct



Optional process A is executed. Condition B is then evaluated. If found to be false, optional process C is executed and control is passed to process A. Condition B is then evaluated again. If condition B is true, then control is passed out of the loop.

Figure 6. LOOP Construct

E.2.4 Naming Conventions

Object, function, and procedure names should be chosen so as to enhance the readability and intelligibility of the program. Insofar as possible, identifiers should be selected so that their parts of speech represent their use, such as nouns to represent objects, verbs to represent functions, etc.. In addition, names used in code and in documentation should be consistent, and all names should be unique.

Language keywords should not be used as names of objects, functions or procedures, or in any manner not consistent with the design of the language.

E.2.5 Coding Conventions

In developing source code, coding conventions should be consistent among all units. Uniform calling sequences should be used, and all parameters should be validated for type and range on entry into each unit.

All source code should be indented to clearly indicate logical levels. Each line of source code should contain no more than one executable statement.

Mixed-mode operations should be avoided. If it is necessary to use them, then their use should be identified by comments.

Separate and consistent formats should be used to distinguish between normal status messages and error or exception messages. They should be self-explanatory, and they should not require the operator to perform any function or look-up to interpret them.

E.2.6 Comments

Comments should be formatted in a uniform manner. Prologue comments should be used to describe:

- the purpose of the unit and how it works;
- other units called and the calling sequence;
- inputs and outputs;
- file references by name and method of access (read, write, modify, append, etc.);
- the use of global and local variables; and
- date of creation and a revision record.

Descriptive comments should be provided to identify objects and data types.

In-line comments should be provided to facilitate interpretation of functional operations, tests and branching.

E.3 Content of Executable Modules

It is recommended that source code modules be organized so that they may be edited to comply with individual state laws, such that no extraneous code not required by a state is installed.

E.4 Optional Audit Records

Optional audit record and vote tally data entries represent additional software features that are not considered to be critical to acceptable system performance. These features would, however, enhance the professionalism of elections operations, contribute to timeliness, and ultimately lead to increased levels of public confidence in the process.

In addition to the required in-process audit record entries, the system may provide a system generated log of every operator interaction with the system or device (in contrast to operator compiled accountability reports). This log should begin with installation and acceptance testing, maintenance activities, and pre-election test actions (whenever tests are run, plus an indication of whether or not such audits were error-free), and proceed through actual election-day processing, subsequent processing updates, and recounts.

Optional vote tally data items would assist the election official in canvassing the votes, analyzing the election, and providing information to the press or the public. They include:

- Percentages for candidate/measure votes, blanks, undervotes, and overvotes;
- The listing of candidates on precinct or summary reports by rank order of vote totals;
- The reported vote totals of candidates within each contest, in rank order of finish; and
- By precinct, the quantity of actual straight party ticket votes (if such votes are permissible under state law).

E.5 Voter Confirmation in DRE Systems

Some jurisdictions may find the incorporation of a voter confirmation capability in DRE systems is advantageous. Voter confirmation provides voters with further indication that the voting device recognizes their choices. If the confirmation is produced as a physical record, that record may also be used in recounts in the same manner that paper ballots in P&M systems are used.

Voter confirmation does not, however, guarantee that the voter choices are correctly recorded and updated in memory registers. Instead, DRE system accuracy and integrity is best safeguarded by adequately testing the implementation of the requirements for multiple memories and a separate processing path for retention of ballot images.

The voter confirmation capability may be implemented using the same data processing path that provides for the capture and retention of ballot images. After a voter has made all voting selections, the DRE machine should display or print on a paper ballot a summary of the voter's selections. If the voter is not satisfied with the confirmation, election workers must have a method of voiding the ballot.

If a printed ballot is produced, it should be in a machine readable format and a ballot box must be provided for the deposit of the record after the voter views it. The user jurisdiction must adhere to administrative procedures necessary to ensure that no voter leaves the polls with the printed record, lest it be used for illegal purposes.

Appendix F

Qualification and Acceptance Test Design Criteria

Appendix F

Qualification and Acceptance Test Design Criteria

F.1 Introduction

Qualification tests are designed to demonstrate that the system meets or exceeds the requirements of the standards. The tests are also used to demonstrate compliance with other levels of performance claimed by the manufacturer. Acceptance tests are conducted to confirm that the units delivered perform at least as well as the unit which was qualified and that they comply with the requirements specified by the local jurisdiction in their procurement document.

Qualification and acceptance tests must satisfy two separate and possibly conflicting sets of considerations. The first is the need to produce enough test data to provide confidence in the validity of the test and its apparent outcome. The second is the need to achieve a meaningful test at a reasonable cost, and cost varies with the difficulty of simulating expected real-world operating conditions and with test duration. It is the test designer's job to achieve an acceptable balance of these constraints.

The rationale and statistical methods of the test designs contained in the standards are discussed below. Technical descriptions of their design can be found in any of several books on testing and statistical analysis.

F.2 Approach to Test Design

The qualification and acceptance tests specified in the standards are primarily concerned with assessing the magnitude of random errors. They are also, however, capable of detecting bias errors that would result in the rejection of the system.

Test data typically produce two results. The first is an estimate of the true value of some system attribute such as speed, error rate, etc. The second is the degree of certainty that the estimate is a correct one. The estimate of an attribute's value may or may not be greatly affected by the duration of the test. Test duration, however, is very important to the degree of certainty; as the length of the test increases, the level of uncertainty decreases. An efficient test design will produce enough data over a sufficient period of time to enable an estimate at the desired level of confidence.

There are several ways to design tests. One approach involves the preselection of some test parameter, such as the number of failures or other detectable factor. The essential element of this type of design is that the number of observations is independent of their results. The test may be designed to terminate after 1,000 hours or 10 days, or when 5 failures have been observed. The number of failures is important because the confidence interval (uncertainty band) decreases rapidly as the number of failures increases. However, if the system is highly reliable or very accurate, the length of time required to produce a predetermined number of failures or errors using this method may be unachievably long.

Another approach is to determine that the actual value of some attribute need not be learned by testing, provided that the value can be shown to be better than some level. The test would not be designed to produce an estimate of the true value of the attribute but instead to show, for example, that reliability is at least 123 hours or the error rate is no greater than one in one million.

The latter design approach, which was chosen for the standards, uses what is called Sequential Analysis. Instead of the test duration being fixed, it varies depending on the outcome of a series of observations. The test is terminated as soon as a statistically valid decision can be reached that the factor being tested is at least as good as or no worse than the predetermined target value. A sequential analysis test design called the "Wald Probability Ratio Test" is used for reliability and accuracy testing.

F.3 Probability Ratio Sequential Test (PRST)

The design of a Probability Ratio Sequential Test (PRST) requires that four parameters be specified:

H0, the null hypothesis
H1, the alternate hypothesis

a, the Producer's risk
b, the Consumer's risk

The standards anticipate using the PRST for testing both time-based and event-based failures.

This test design provides decision criteria for accepting or rejecting one of two test hypotheses: the null hypothesis which is the Nominal Specification Value (NSV) or the alternate hypothesis which is the MAV. The MAV could be either the Minimum

Acceptable Value or the Maximum Acceptable Value depending upon what is being tested.[1]

In the case of Mean Time Between Failure (MTBF), for example, the null hypothesis is that the true MTBF is at least as great as the desired value (NSV), while the alternate hypothesis is that the true value of the MTBF is less than some lower value (Minimum Acceptable Value). In the case of error rate, the null hypothesis is that the true error rate is less than some very small desired value (NSV), while the alternate hypothesis is that the true error rate is greater than some larger value which is the upper limit for acceptable error (Maximum Acceptable Value).

F.4 Time-based Failure Testing Criteria

An equivalence between a number of events and a time period can be established when the operating scenarios of a system can be determined with precision. Many of the performance test criteria of Section 7, Qualification Test and Measurement Procedures, use this equivalence (specifically, the tests for hardware and systems-level reliability). Acceptance tests might also incorporate such extended operations testing but would not use the environmental test chamber required during hardware qualification testing.

System acceptance or rejection can be determined by observing the number of relevant failures which occur during equipment operation. The probability ratio for this test is derived from the Exponential probability distribution. This distribution implies a constant hazard rate. Therefore, two or more systems may be tested simultaneously to accumulate the required number of test hours, and the validity of the data is not affected by the number of operating hours on a particular unit of equipment. However, for environmental operating hardware tests, no unit shall be subjected to less than two complete 24 hour test cycles in a test chamber as required by Subsection 7.3.3.2. of the standards.

In this case, the null hypothesis is that the Mean Time Between Failure (MTBF), as defined in Subsection 3.4.3 of the standards, is at least as great as some value, here the Nominal Specification Value. The alternate hypothesis is that the MTBF is no better than some value, here the Minimum Acceptable Value.

For example, a typical system operations scenario for environmental operating hardware tests will consist of approximately 45 hours of equipment operation. Broken down, this time allotment involves 30 hours of equipment set-up and readiness testing and 15 hours of elections operations. If the Minimum Acceptable Value is defined as

---

1/ Performance may be specified by means of a single value or by two values. When a single value is specified, it shall be interpreted as an upper or lower single-sided 90 percent confidence limit. If two values, these shall be interepreted as a two-sided 90 percent confidence interval, consisting of the NSV and MAV.

45 hours, and a test discrimination ratio of 3 is used (in order to produce an acceptably short expected time of decision), then the Nominal Specification Value equals 135 hours.

With a value of decision risk equal to 10 percent, there is no more than a 10 percent chance that a system would be rejected when, in fact, with a true MTBF of at least 135 hours, the system would be acceptable. It also means that there is no more than a 10 percent chance that a system would be accepted with a true MTBF lower than 45 hours when it should have been rejected.

Therefore,

H0: MTBF = 135 hours
H1: MTBF = 45 hours

a = 0.10
b = 0.10

and the minimum time to accept (on zero failures) is 163 hours.

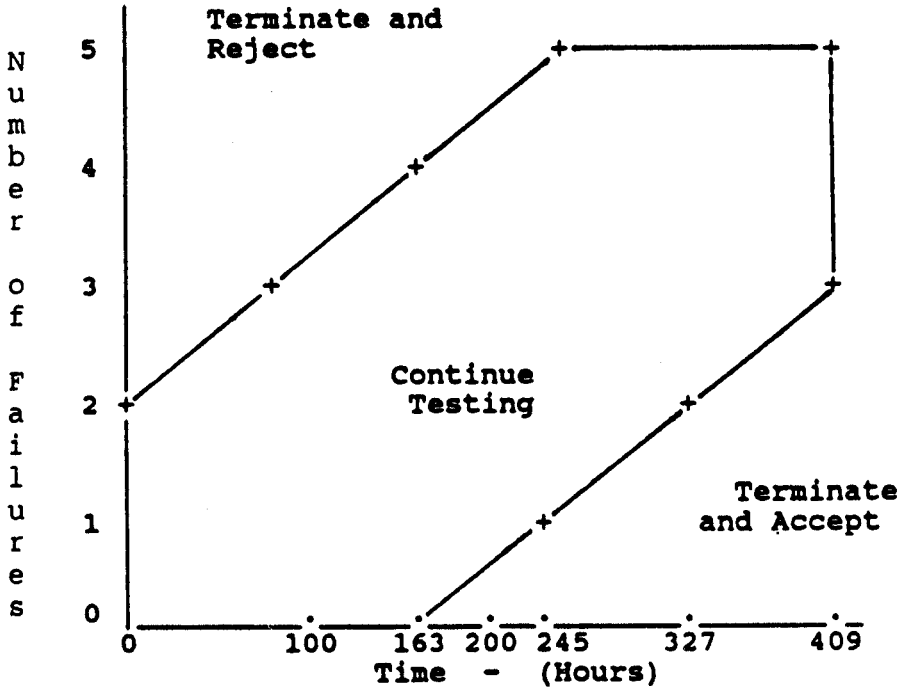
It follows, then, that the test is terminated and an ACCEPT decision is reached when the cumulative number of equipment hours in the second column of the following table has been reached, and the number of failures is equal to or less than the number shown in the first column. The test is terminated and a REJECT decision is reached when the number of failures occurs in less than the number of hours specified in the third column. In the event that no decision has been reached by the times shown in the last table entries, the test is terminated, and the decision is declared as indicated.

Number of Failures	Accept if Time Greater Than	Reject if Time Less Than
0	163	Continue test
1	245	Continue test
2	327	Continue test
3	409 (1)	82
4		163
5		245 (2)

(1) Terminate and ACCEPT
(2) Terminate and REJECT

The ACCEPT/REJECT criteria of this time-based test accommodate the inclusion of partial failures (as defined in Appendix H) in the following manner. A graph is drawn, consisting of two parallel lines through the sets of numbers of failures and time values shown in the table. These lines are plotted against the total number of failures on the

vertical axis, and the elapsed time on the horizontal axis. They become "ACCEPT" and "REJECT" boundaries. As an illustration, the graph shown below has been constructed using the values from the previous table.



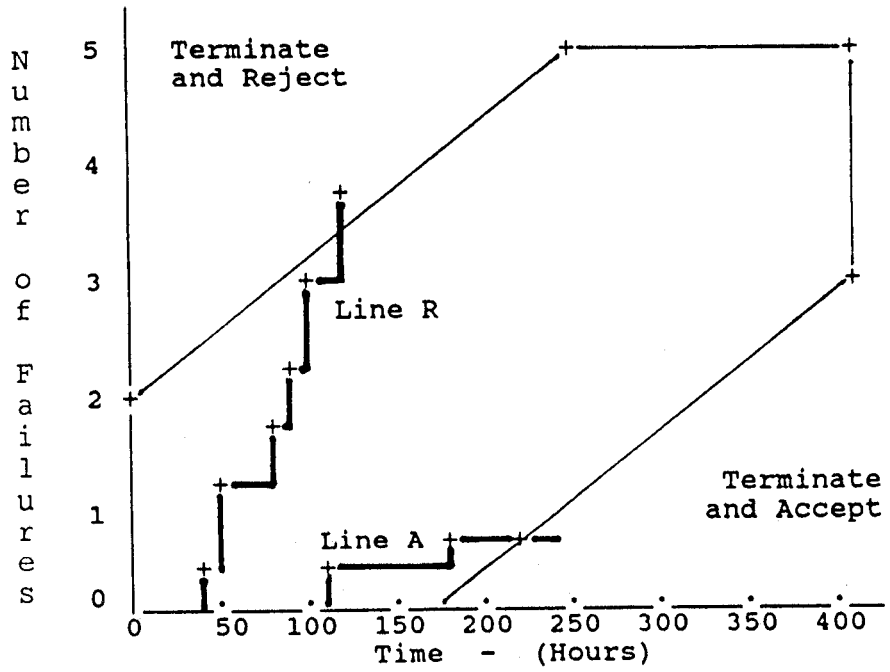
As operating time is accrued, the horizontal line is extended from the origin to the current value of time. If a total or partial failure occurs, the value of the cumulative failure score is plotted at the time when the failure occurred. A vertical line is drawn between this point and the horizontal trace. The test is resumed and the horizontal trace is continued at the level of the cumulative failure score.

The test is terminated and the equipment is accepted whenever this horizontal line intersects the lower of the two parallel lines. If the vertical line drawn to connect the horizontal trace to the new cumulative failure score intersects the upper of the two parallel lines, the test is terminated and the equipment rejected.

The test is terminated and the equipment is rejected if a total score of 5.0 or more is reached. If after 409 hours of operation the cumulative failure score is less than 5.0, than the equipment is accepted.

For example, assume that System R experienced a sequence of partial failures as shown in the table below. The system would be rejected after the sixth failure event because its operating trace intersected the upper boundary. Similarly, System A would be accepted when its operating trace intersected the lower boundary at 220 hours.

System R			System A		
Time	Score	Cum. Score	Time	Score	Cum. Score
34	0.5	0.5	123	0.5	0.5
45	0.8	1.3	189	0.2	0.7
78	0.5	1.8	220	-	0.7
89	0.5	2.3			
101	0.8	3.1			
123	0.5	3.6			



F.5 Event-based Failure Testing Criteria

Some voting system performance attributes are tested by inducing an event or series of events, and the relative or absolute time intervals between repetitions of the event has no significance. Although an equivalence between a number of events and a time period can be established when the operating scenarios of a system can be determined with precision, another type of test is required when such equivalence cannot be established. It uses event-based failure frequencies to arrive at ACCEPT/REJECT criteria. This test may be performed simultaneously with time-based tests.

For example, the failure of a switch is usually dependent on the number of times that it is actuated. The elapsed time over which a certain number of actuation cycles occurs is, under most circumstances, not important. Another example of such an attribute is the frequency of errors in reading, recording, and processing vote data. This frequency, called "bit error rate," applies to such functions as the binary process of detecting the presence or absence of a voting punch or mark, or to the closure of a switch corresponding to the selection of a candidate.

Qualification and acceptance test procedures that accommodate event-based failures are, therefore, based on a discrete, rather than a continuous probability distribution. A Probability Ratio Sequential Test using the binomial distribution is recommended. In the case of system error rate:

H0: Desired error rate = 1 in 10,000,000
H1: Maximum acceptable = 1 in 100,000

a = 0.05
b = 0.05

and the minimum error-free sample size to accept for qualification tests is 297,589 votes.

The nature of the problem may be illustrated by the following example, using the criteria contained in the standards for system error rate. A target for the desired accuracy is established at a very low error rate. A threshold for the worst error rate that can be accepted is then fixed at a somewhat higher error rate. Next, the decision risk is chosen, that is the risk that the test results may not be a true indicator of either the system's acceptability or unacceptability. The process is as follows:

- The desired accuracy of the voting system, whatever its true error rate (which may be far better), is established as no more than one error in every ten million votes counted.

- If it can be shown that the system's true error rate does not exceed one in every one hundred thousand votes counted, it will be considered accept-

able. (This is more than accurate enough to declare the winner correctly in almost every election.)

- A decision risk of 5 percent is chosen, to be 95 percent sure that the test data will not indicate that the system is bad when it is good or good when it is bad.

This results in the following decision criteria:

- If the system makes one error before counting 167,753 consecutive votes correctly, it will be rejected.

- If the system reads at least 297,589 consecutive votes correctly, it will be accepted.

- If the system correctly reads more than 167,753 votes but less than 297,589 when the first error occurs, the testing will have to be continued until another 465,342 consecutive votes are counted without error (a total of 762,763 with one error).

This test design replaces the horizontal axis in the time-based illustrations with the total number of trials. Just as there was a minimum time to accept without failure, there will be a minimum data sample size to accept without error. As a practical matter, the test is terminated if an error occurs in less than 167,753 votes. The vendor is then required to improve the system.

F.6 Resolving Discrepancies During Data Accuracy Testing

Data accuracy criteria for qualification and acceptance tests are intended to demonstrate that the system meets at least the minimum accuracy requirements established by the standards. Ballots for this test may be of any format which is capable of generating a large number of voting marks in each counting cycle. Ballot-reading logic capability is not exhaustively tested by the procedure.

In the event of discrepancy among the totals for any ballot position obtained on each of the ballot-counting cycles, or among the sums of the totals for all of the ballot positions, the following procedure shall apply:

Step 1 For each ballot position, compute the difference between the largest and the smallest totals.

Step 2 Sum the differences for all ballot positions.

Step 3 Sum the totals for all ballot positions on each counting cycle.

Step 4 Compute the sum of all ballot positions on all counting cycles.

Step 5 Compute the ratio of the sum of the differences from Step 2 to the sum of all votes from Step 4.

Step 6 If the ratio from Step 5 is less than 1/300,000, then accept the system and terminate the test; otherwise proceed to Step 7.

Step 7 If the ratio from Step 5 is equal to or greater than 1/167,000, then reject the system; otherwise proceed to Step 8.

Step 8 If the testing agency and the vendor agree that the cause of the discrepancy can be identified and corrected, and if this corrective action is taken, then repeat the test in its entirety; otherwise, reject the system.

F.7 Alternative Test Criteria

Correct counting of votes is an essential element of all voting systems. Testing permits the evaluation of whether or not voting systems count and report votes correctly. It would, of course, be desirable that voting systems have an error rate of zero; they would never make a mistake regardless of the number of ballots counted. If this had to be proven by a test, however, the test would take an infinity of time. Therefore, the accuracy rate required by the standards was established as a reasonable compromise between desired accuracy and projected time and expense of testing.

The test design would be dramatically changed if 1 in 100,000 were considered to be too high a true error rate and a lower rate, such as 1 error in 1,000,000, were required. Instead of accepting the system if it accumulated 297,589 consecutive votes without error, the system would be required to count 3,271,600 votes without error. Such a test would be about eleven times longer (and more costly). The potential benefit of such extensive testing is not considered to be worth the added cost.

If a less rigorous threshold were required, such as one with a desired error rate reduced from 1 in ten million to 1 in one million while maintaining the maximum true error rate at 1 in 100,000, a shorter but less reliable test could be conducted. A system could be accepted after only 11,111 consecutive counts without error, a test approximately 1/20th the duration of the test now required by the standards. This test, however, would not provide the necessary level of assurance that a defective system would not find its way into the marketplace. The cost/risk trade-off of this approach is, therefore, not considered acceptable.

Appendix G

Voting System Failure Definition and Scoring Criteria

Appendix G

Voting System Failure Definition and Scoring Criteria

G.1 Introduction

G.1.1 Purpose and Scope

The purpose of this Appendix is to provide a uniform means of assessing voting system performance during qualification and acceptance testing, by identifying failure modes that have a critical effect upon system operation, those that permit continued operation of the system (albeit in a degraded fashion, or with reduced capability), and those that can be readily corrected without significant impact on either the preparation for or the conduct of an election.

The emphasis of this Appendix is upon identifying failure modes which may result in the loss of a critical performance attribute, or in the loss or corruption of voting data. These failures are defined below as "total" failures. They are so important as to require that testing procedures be interrupted if they occur, so that they can be corrected. The effectiveness of the corrective action must be verified by ancillary tests before the qualification or acceptance tests may be resumed.

The failure classification method also makes provision for recording the frequency of events that have no significant bearing on system operation. These events contribute to the overall maintenance burden, both in down-time and in corrective maintenance man-hours. All interruptions of service shall be recorded, along with the time, and number of personnel required to correct the failure condition.

This Appendix does not provide failure definitions or scoring criteria for source code inspection.

G.1.2 Failure Definitions

Any failure to perform a system function correctly, or any data error which occurs during a qualification or acceptance test, shall be recorded. However, the event will not be classified as a relevant failure if at least one of the following conditions is present:

- the equipment was improperly prepared for the test;
- an improper procedure was performed; or
- the defect resulted from the failure of an external device.

The term "equipment" is inclusive of computer programs installed in or resident in devices which comprise the system. The operation of devices is understood to mean the operation of both hardware and software. The term "defect" refers to a failure to operate or operate correctly, whether due to hardware or software.

G.2 Failure Classification

Any defect or malfunction that occurs during equipment operation shall be recorded and classified according to the following criteria.

Step	Decision Criterion	Classification
(1)	Is the defect the result of an error in manufacturing or documentation?[1]	If YES Non-Relevant
(2)	Is the defect the result of a failure of a piece of test equipment (not the device under test)?	If YES Non-Relevant
(3)	Is the defect the result of an error in the application of a test procedure?	If YES Non-Relevant
(4)	Is the defect the result of human error in the performance of an operational procedure, and is there an immediate audible or visual alarm?	If YES Non-Relevant
(5)	Is the defect a secondary failure not involving loss of data?	If YES Non-Relevant

1/ If the qualification test must be interrupted, and corrective action cannot be successfully taken as defined in Subsection 7.2.4, then the test will be terminated, and the equipment rejected.

Step	Decision Criterion		Classification
(6)	Can the equipment be restored to a fully operational status without any loss of data in the time allowed?	If YES	Non-Relevant
(7)	Otherwise, the defect is		RELEVANT

G.3 Failure Scoring

A relevant failure shall be assessed according to its effect on the ability of the system to respond to an operational demand, or to complete its intended functions. The system shall be required to satisfy the demands of three principal election phases, namely:

- pre-voting operations
- voting operations
- post-voting operations

The criteria for assessing the probable effect of a failure are both objective and subjective. The failure may receive a Failure Score of 1.0. This means that the particular mode of failure is certain to result in a data error, or in the loss of a critical system function. If such a failure occurs during any portion of the test, the procedure specified in Subsection 7.2.4, Test Evaluation of Performance Criteria, shall be invoked. This procedure defines the action to be taken to resolve and purge the failure.

If a failure has no effect on the accuracy and integrity of voting data, and if its effect can be ameliorated by an alternate mode of operation, or by the substitution of a redundant or spare item of equipment, then the effect is a "degraded" mode of operation. Loss of function is not certain; therefore, a failure score less than 1.0 may be assigned. The event is classified as a "partial," as opposed to a total, failure. The score assigned to the partial failure is an estimate of the reduction in system effectiveness due to it, or of the likelihood that a subsequent loss of the alternate mode or spare may occur before completion of the function.

G.4 Functional Failures and Scores

The phases of elections operations, defined in Subsection G.3, are expanded in this section to identify typical functional failures that may affect the successful performance of the operations.

The consequence of a failure may depend upon when it occurs. For example, the time allowable to correct a failure during the set-up of a polling place voting device may be several hours. During voting, the time allowable to correct the same failure may be several minutes. The specification of criteria, and the assignment of failure scores, reflect both the local and global effects of the failure.

Care must be taken to ensure that the cause of failure is correctly and uniformly classified by the criteria of Subsection G.2. However, the definitions are not exhaustive. If a failure cannot be classified according to one of the following definitions, then the test agency shall make its own assessment of the consequence of failure, and assign an appropriate score.

G.4.1 Pre-voting Operations

Pre-voting operations include all functions required to plan for and initiate an election.

G.4.1.1 Equipment Activation

Voting device and test equipment activation consists of all operations required to prepare central and polling place equipment for election use. These operations include removal from storage, cleaning and maintenance operations, resupply of consumables, and verification of operational status. Any inability to perform one or more of these functions constitutes a failure. Examples include: failure to commence operation when power is applied, failure of displays or indicators to respond to changes in system status, failure of switches or control devices, and inability to support readiness tests and report generation.

Defect	Score
Total Loss of Function: Any defect which results in the inability of the equipment to enter an operational condition when power is applied, or the inability to complete any prescribed diagnostic or maintenance task, and which requires more than 4 hours for correction and verification.	1.0
Partial Failure, Degraded Operation: Any defect, as defined above, that results in corrective maintenance requiring 1 to 4 hours for correction and verification.	0.2
No Effect on Function: Any functional failure which is the result of human error. Any defect which can be corrected and verified within 1 hour.	0.0

G.4.1.2 Election Planning and Preparation

Election preparation includes:

- the definition of offices and measures which are to appear on the ballot, and the names of candidates for each office;
- the definition of district and sub-district boundaries, and the associated offices and issues;
- the establishment of the number and arrangement of individual ballot formats required to accommodate applicable election law;
- the construction and linking of the election and associated administrative databases with data entry, processing, and retrieval (linking the external environment with the tally system); and
- the generation of input and output data and system status reports in the required formats.

It also incorporates the implementation of administrative and security control and audit procedures that apply to this and succeeding phases of the election.

Defect	Score
Total Loss of Function: Any defect that results in the: • inability to activate system application programs and data structures; • inability to define the content of the election, and the various ballot formats required by local election laws; • inability to integrate election software and data with related external application programs and data; • inability to generate error-free reports; or • inability to enable and support testing required to validate the successful installation and operation of these functions; and that requires more than 4 hours for correction and verification of the corrective action.	1.0

Partial Loss of Function, Degraded Operation: There are no degraded modes of operation for this function. All system operations must be successfully completed, and all operating procedures and controls must be installed and adhered to.

No Effect on Function: Any functional failure that is the result of human error. Any defect that can be corrected and verified within 4 hours. 0.0

G.4.1.3 Election Programming

Election programming consists of all action required to install programs that enable and control equipment operation during election use. This function includes the verification of resident programs, the installation of software or firmware which is unique to the election, the testing of all programs, and the generation of data reports, and reports of operating computer program and equipment status.

Defect	Score

Total Loss of Function: Any defect that: 1.0

- prevents the installation of software, firmware or ballot display materials;
- prevents the completion of programming required to set up the equipment for a specific election;
- prevents the successful completion of pre-election logic and accuracy tests; or
- prevents the generation of data and audit reports;

and that requires more than 1 hour for correction and verification.

Partial Failure, Degraded Operation: Any defect, as defined above, that requires between 15 minutes and 1 hour for correction and verification. 0.2

No Effect on Function: Any defect that can be corrected and verified in less than 15 minutes. 0.0

G.4.2 Voting Operations

Voting operations include all functions required to open the polling place, enable ballots, and record votes.

G.4.2.1 Opening the Polling Place

These functions include all operations required to install voting equipment in the polling place, and to verify its readiness for use by voters.

Defect	Score
Total Loss of Function: Any defect that: • results in the inability of the equipment to enter an operational condition when it is installed in the polling place; • prevents the successful completion of any prescribed diagnostic or maintenance task; • prevents the completion of routines performed before vote recording, such as obtaining an equipment status and signature form, and a "Zero Printout" record; or • prevents opening of the polling place; and that requires more than 15 minutes for correction and verification.	1.0
Partial Failure, Degraded Operation: There are no degraded modes of operation for this function. All polling place equipment must be capable of operation in all intended operating modes prior to opening of the polls.	
No Effect on Function: Any defect that can be corrected and verified within 15 minutes.	0.0

G.4.2.2 Enabling Ballots and Recording Votes

This function includes all operations and capabilities required to enable the full and correct ballot upon which each voter is entitled to vote, to correctly record the selections of the voter, and to cast or produce the voted ballot.

Defect	Score
Total Loss of Function: Any defect in P&M system that: • prevents the voter from registering a vote for the candidate or issue of choice;	1.0

- prevents the registering of a write-in vote;
- prevents the casting of a voted ballot;
- results in a condition which makes a ballot unreadable, unless caused by a deliberate act of the voter; or
- violates the privacy and security of the ballot;

and that requires more than 10 minutes for correction and verification.

Any defect in DRE systems that:

- prevents the designation of party preference in a Primary Election;
- prevents the enabling of the equipment for voting;
- disables the selection of any legitimate voting choice;
- fails to signal an attempt to select an illegitimate voting choice;
- disables the function and capability of casting a write-in vote;
- results in failure to accept a legitimately voted ballot;
- violates the privacy and security of the ballot; or
- results in the loss or corruption of previously recorded ballot data;

and that requires more than 10 minutes for correction and verification.

Partial Failure, Degraded Operation: Any defect not involving the loss or corruption of voting data, for which an alternate operating mode or active standby device is not available, and that can be corrected and verified in less than 30 minutes. 0.8

Partial Failure, Degraded Operation: Any defect not involving the loss or corruption of voting data that results in entry into an 0.4

alternate or redundant operational mode, or the selection of an active standby device.

No Effect on Function: Any defect not involving the loss or corruption of voting data, that can be corrected and verified in less than 10 minutes. 0.0

G.4.2.3 Central Counting Operations

This function includes all operations and capabilities required to count ballots or to accumulate the results of previously counted ballots at one or more central counting places, to merge the voting data produced by dissimilar systems, to merge ballots or voting results from manually processed ballots, to program or reprogram ballot counting devices after opening of the polling places, or to edit vote counting programs or voting data.

Defect	Score

Total Loss of Function: Any defect that results in: 1.0

- inability to count ballots;
- inability to process voting data from programmable memory devices or other voting data transfer media;
- inability to merge or edit voting data;
- a processing error in an output report; or
- inability to produced the required type and quantity of output reports.

Partial Failure, Degraded Operation: Any defect that is not a total failure but which impedes the completion of central counting operations in a timely manner, or that requires the intervention of a maintenance technician. 0.5

No Effect on Function: Any defect that does not result in a total or partial failure, or which can be corrected by the equipment operator or system manager. 0.0

G.4.3 Post-voting Operations

Post-voting operations include all functions required to close the polling place, obtain reports of audit and vote data, and preserve vote data and documentation.

G.4.3.1 Closing the Polling Place

This function includes all operations and capabilities required to disable further voting after the close of the polling place, and to enable or generate all status, audit, and data reports required to be produced at the polling place.

Defect	Score
Total Loss of Function: Any defect that: • results in inability to close the polling place; • results in inability to obtain the desired number of output reports; • produces an error in the production of an output report; or • causes an irrecoverable loss or corruption of any portion of the voting data.	1.0
Partial Failure, Degraded Operation: Any defect not involving the loss or corruption of voting data that requires more than 15 minutes for corrective maintenance and verification.	0.6
No Effect on Function: Any defect not resulting in the loss or corruption of voting data, and that can be corrected and verified in less than 15 minutes.	0.0

G.4.3.2 Obtaining Reports

This function includes all operations and capabilities necessary to consolidate voting data from all voting devices and polling places, to process absent voter ballots and any other ballots which require exceptional handling, to produce voting data reports, and other reports associated with the results of the election.

Defect	Score
Total Loss of Function: Any failure to correctly process voting data, audit data and administrative data at any level of reporting, or to support testing required to validate these operations.	1.0
Partial Loss of Function, Degraded Operation: Any failure to correctly process and report non-voting data, provided that the defect can be corrected and verified in no more than 1 hour.	0.5

Defect	Score
No Effect on Function: Any failure not affecting the ability to process data, or to generate standard or special reports.	0.0

G.4.3.3 Retaining Data and Documentation

This function includes the handling, transportation, conditioning, and storage of voting system equipment, supplies, and computer programs to preserve required vote data and documentation.

Defect	Score
Total Loss of Function: Any loss or corruption of voting or audit record data or deterioration of ballots, inability to recover data, or produce a report of voting data that occurs during the 6-month period for recounts and contested elections.	1.0
Partial Failure, Degraded Operation: Any defect occurring during, or as a result of, storage and transportation, not involving a total loss of function as defined above, that requires more than 4 hours of correction and verification.	0.4
No Effect on Function: Any defect occurring during, or as a result of, storage and transportation, not involving a total loss of function as defined above, that can be repaired and verified within 4 hours.	0.0

Appendix H

Qualification Test Plan

Appendix H

Qualification Test Plan

This Appendix contains a recommended outline for the Qualification Test Plan, which is to be prepared by the test agency. The primary purpose of the test plan is to document the test agency's development of the complete or partial qualification test. A sample outline of a Qualification Test Plan is illustrated on Page H-12.

It is intended that the test agency use this Appendix as a guide in preparing a detailed test plan, and that the scope and detail of the requirements for qualification be tailored to the type of hardware, and the design and complexity of the software being tested. Required hardware tests are defined in Section 7, whereas software and system-level tests must be developed based on the vendor prequalification tests and information available on the specific software's physical and functional configuration.

Prior to development of any test plan, the test agency must obtain the Technical Data Package (TDP) from the vendor submitting the voting system for qualification. The TDP contains information necessary to the development of a Qualification Test Plan, such as the vendor's Hardware Specifications, Software Specifications, System Operating Manual and System Maintenance Manual. See Appendix B.

It is foreseen that vendors may submit some voting systems in use at the time the standards are issued to partial qualification tests. It is also specified by the standards that voting systems incorporating the vendor's software and off-the-shelf hardware need only be submitted for software and system-level tests. Requalification of systems with modified software or hardware is also anticipated. The test agency shall alter the test plan outline as required by these situations.

H.1 Introduction

The test agency shall include the identification, and a brief description of, the hardware and software to be tested, and any special considerations which affect the test design and procedure.

H.1.1 References

The test agency shall list all documents that contain material used in preparing the test plan. This list shall include specific reference to applicable portions of the standards, and to the vendor's Hardware Specifications and Software Specifications.

H.1.2 Terms and Abbreviations

The test agency shall list and define all terms and phrases relevant to the hardware, the software, or the test plan.

H.2 Prequalification Tests

H.2.1 Prequalification Test Activity

The test agency shall evaluate vendor tests, or other agency tests in determining the scope of testing required for system qualification. Prequalification tests may be particularly useful in designing of software functional test cases.

H.2.2 Prequalification Test Results

The test authority shall summarize prequalification test results which support the discussion of the preceding section.

H.3 Materials Required for Testing

H.3.1 Software

The test authority shall list all software required for the performance of hardware, software, and system tests. If the test environment requires supporting software such as operating systems, compilers, assemblers, or database managers, then this software shall also be listed.

H.3.2 Equipment

The test authority shall list all equipment required for the performance of the hardware, software, and system tests. This list shall include system hardware, general purpose data processing equipment, and test instrumentation, as required.

H.3.3 Test Materials

The test authority shall list all test materials required in the performance of the test including, as applicable, test ballot layout and generation materials, test ballot sheets,

test ballot cards and control cards, standard and optional output data report formats, and any other materials used to simulate preparation for and conduct of elections.

H.3.4 Deliverable Materials

The test authority shall list all documents and materials to be delivered as a part of the system, such as:

- hardware specification;
- software specification;
- voter, operator, and hardware and software maintenance manuals;
- program listings, facsimile ballots, tapes; and
- sample output report formats.

H.3.5 Proprietary Data

The test authority shall list and describe all documentation and data that are the private property of the vendor, and hence are subject to restrictions with respect to test authority use, release, or disclosure.

H.4 Test Specifications

H.4.1 Requirements

The test authority shall cite the pertinent hardware qualitative examinations and quantitative tests which follow from Sections 3 and 7 of the standard. The test authority shall also describe the specific test requirements which follow from the design of the software under test.

The qualification test shall include ITA consideration of hardware and software design; and ITA development and conduct of all tests to demonstrate satisfactory performance. Environmental, non-operating tests shall be performed in the categories of simulated environmental conditions specified by the vendor or user requesting the tests. Environmental operating tests shall be performed under varying temperatures. Other functional tests shall be conducted in an environment that simulates, as nearly as possible, the intended use environment.

Test hardware and software shall be identical to that designed to be used together in the voting system, except that software intended for use with general-purpose off-the-

shelf hardware may be tested using any equivalent equipment capable of supporting its operation and functions.

H.4.2 Hardware Configuration and Design

The test authority shall document the hardware configuration and design in detail sufficient to identify the specific equipment being tested. This document shall provide a basis for the specific test design and include a brief description of the intended use of the hardware.

H.4.3 Software System Functions

The test authority shall describe the software functions in sufficient detail to provide a foundation for selecting the test case designs and conditions contained in Subsections H.4.4.3, H.4.4.4, and H.4.4.5, below. On the basis of this test case design, the test authority shall prepare a table delineating software functions and how each shall be tested.

H.4.4 Test Case Design

H.4.4.1 Hardware Qualitative Examination Design

The test authority shall review the results, submitted by the vendor, of any previous examinations of the equipment to be tested. The results of these examinations shall be compared to the performance characteristics specified by Section 2 of the standards concerning the requirements for:

- pre-voting functions
- voting functions
- post-voting functions

In the event that a review of the results of previous examinations indicates problem areas, the test agency shall provide a description of further examinations required prior to conducting the environmental and system-level tests. If no previous examinations have been performed, or records of these tests are not available, the test agency shall specify the appropriate tests to be used in the examination.

H.4.4.2 Hardware Environmental Test Case Design

The test authority shall review the documentation, submitted by the vendor, of the results and design of any previous environmental tests of the equipment submitted for testing. The test design and results shall be compared to the Qualification Test and Measurement Procedures, Section 7 of the standards. The test agency shall cite any additional tests required, based on this review and those tests requested by the

vendor or the state. The test agency shall also cite any environmental tests of Section 7 that are not to be conducted, and note the reasons why.

For complete qualification, environmental tests shall include the following tests, depending upon the design and intended use of the hardware.

- Non-operating tests, including the:

  (a) transit drop test
  (b) bench handling test
  (c) vibration test
  (d) low temperature test
  (e) high temperature test
  (f) humidity test
  (g) rain exposure test (if applicable)
  (h) sand and dust exposure test (if applicable)

- Operating tests involving a series of procedures that test system reliability and accuracy under various temperatures and voltages relevant to election use.

H.4.4.3 Software Module Test Case Design and Data

The test agency shall review the vendor's program analysis, documentation, and, if available, module test case design. The test agency shall evaluate the test cases for each module, with respect to flow control parameters and data on both entry and exit. All discrepancies between the Software Specifications and the test case design shall be corrected by the vendor prior to initiation of the qualification test.

If the vendor's module test case design does not provide conclusive coverage of all program paths, then the test agency shall perform an independent analysis to assess the frequency and consequence of error of the untested paths. The test authority shall design additional module test cases, as required, to provide coverage of all modules containing untested paths with potential for untrapped errors.

The test agency shall also review the vendor's module test data in order to verify that the requirements of the Software Specifications have been demonstrated by the data. In the event that the vendor's module test data are insufficient, the test agency shall provide a description of additional module tests, prerequisite to the initiation of functional tests.

H.4.4.4 Software Functional Test Case Design

The test agency shall review the vendor's test plans and data to verify that the individual performance requirements described in the Functional Specifications

section of the Software Specifications (see Appendix B, Subsection B.3.3.5) are reflected in the software.

As a part of this process, the test agency shall review the vendor's functional test case designs. The test agency shall prepare a detailed matrix of system functions and the test cases that exercise them. The test agency shall also prepare a test procedure describing all test ballots, operator procedures, and the data content of output reports. Abnormal input data and operator actions shall be defined. Test cases shall also be designed to verify that the system is able to handle and recover from these abnormal conditions.

The vendor's test case design may be evaluated by any standard or special method appropriate; however, emphasis shall be placed on those functions where the vendor data on module development reflects significant debugging problems, and on functional tests that resulted in disproportionately high error rates.

The test agency shall define ACCEPT/REJECT criteria for qualification using the Software Specifications and, if the software runs on special hardware, the associated Hardware Specifications to determine acceptable ranges of performance.

The test agency shall describe the functional tests to be performed. Depending upon the design and intended use of the voting system, all or part of the functions listed below shall be tested.

- Ballot preparation subsystem
- Test operations performed prior to, during, and after processing of ballots, including:
  - (a) Logic tests to verify interpretation of ballot styles, and recognition of precincts to be processed;
  - (b) accuracy tests to verify ballot reading accuracy;
  - (c) status tests to verify equipment statement and memory contents;
  - (d) report generation to produce test output data; and
  - (e) report generation to produce audit data records.
- Procedures applicable to equipment used in the polling place for:
  - (a) opening the polling place and enabling the acceptance of ballots;
  - (b) maintaining a count of processed ballots;

(c) monitoring equipment status;

(d) verifying equipment response to operator input commands;

(e) generating real-time audit messages;

(f) closing the polling place and disabling the acceptance of ballots;

(g) generating election data reports;

(h) transfer of ballot counting equipment, or a detachable memory module, to a central counting location; and

(i) electronic transmission of election data to a central counting location.

- Procedures applicable to equipment used in a central counting place:

(a) initiating the processing of a ballot deck or PMD for one or more precincts;

(b) monitoring equipment status;

(c) verifying equipment response to operator input commands;

(d) verifying interaction with peripheral equipment, or other data processing systems;

(e) generating real-time audit messages;

(f) generating precinct-level election data reports;

(g) generating summary election data reports;

(h) transfer of a detachable memory module to other processing equipment;

(i) electronic transmission of data to other processing equipment; and

(j) producing output data for interrogation by external display devices.

H.4.4.5 System-level Test Case Design

The test agency shall provide a description of system tests of both the software and hardware. For software, these tests shall be designed according the stated design objective without consideration of its functional specification. The test agency shall

independently prepare the system test cases to assess the response of the hardware and software to a range of conditions, such as:

- **volume tests** to investigate the system's response to processing more than the expected number of ballots/voters per precinct, to processing more than the expected number of precincts, or to any other similar conditions which tend to overload the system's capacity to process, store, and report data;

- **stress tests** to investigate the system's response to transient overload conditions. Polling place devices shall be subjected to ballot processing at the high volume rates at which the equipment can be operated to evaluate software response to hardware-generated interrupts and wait states. Central counting systems shall be subjected to similar overloads, including, for systems which support more than one card reader, continuous processing through all readers simultaneously;

- **usability tests** designed to exercise characteristics of the software such as response to input control or text syntax errors, error message content, audit message content, and other features contained in the software design objectives but not directly related to a functional specification;

- **security tests** designed to defeat the security provisions of the system;

- **performance tests** to verify accuracy, processing rate, ballot format handling capability, and other performance attributes claimed by the vendor; and

- **recovery tests** to verify the ability of the system to recover from hardware and data errors.

H.5 Test Data

H.5.1 Data Recording

The test agency shall identify all data recording requirements (e.g.; what is to be measured, how tests and results are to be recorded). The test agency shall also design or approve the design of forms or other recording media to be employed. The test agency shall supply any special instrumentation (pulse measuring device) needed to satisfy the data requirements.

H.5.2 Test Data Criteria

The test agency shall describe the criteria against which test results will be evaluated, such as the following:

- Tolerances: the acceptable range for system performance. These tolerances shall be derived from the hardware performance requirements contained in the applicable sections of the Performance and Testing Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems.

- Samples: the minimum number of combinations or alternatives of input and output conditions that can be exercised to constitute an acceptable test of the parameters involved.

- Events: the maximum number of interrupts, halts or other system breaks which may occur due to nontest conditions. This count shall not include events from which recovery occurs automatically or where a relevant status message is displayed.

H.5.3 Test Data Reduction

The test agency shall describe the techniques to be used for processing test data. These techniques may include manual, semi-automatic, or fully automatic reduction procedures. However, semi-automatic and automatic procedures shall have been shown to be capable of handling the test data accurately and properly. They shall also produce an item-by-item comparison of the data and the embedded acceptance criteria as output.

H.6 Test Procedure and Conditions

The test agency shall describe the test conditions and procedures for performing the tests. If tests are not to be performed in random order, this section shall contain the rationale for the required sequence, and the criteria which must be met, before the sequence can be continued. This section shall also describe the procedure for setting up the equipment in which the software will be tested, for system initialization, and for performing the tests. Each of the following sections that contains a description of a test procedure shall also contain a statement of the criteria by which readiness and successful completion shall be indicated and measured.

H.6.1 Facility Requirements

The test agency shall describe the space, equipment, instrumentation, utilities, manpower, and other resources required to support the test program.

H.6.2 Test Set-up

The test agency shall describe the procedure for arranging and connecting the system hardware with the supporting hardware. It shall also describe the procedure required to initialize the system, and to verify that it is ready to be tested.

H.6.3 Test Sequence

The test agency shall state any restrictions on the grouping or sequence of tests in this section.

H.6.4 Test Operations Procedures

The test agency shall provide the step-by-step procedures for each test case to be conducted. Each step shall be assigned a test step number and this number, along with critical test data and test procedures information, shall be tabulated onto a test report form for test control and the recording of test results.

In this section, the test agency shall also identify all test operations personnel, and their respective duties. In the event that the operator procedure is not defined in the vendor's operations or user manual, the test agency shall also provide a description of the procedures to be followed by the test personnel.

Exhibit H-1 - Test Plan Outline

1	INTRODUCTION
1.1	References
1.2	Terms and Abbreviations
2	PREQUALIFICATION TESTS
2.1	Prequalification Test Activity
2.2	Prequalification Test Results
3	MATERIALS REQUIRED FOR TESTING
3.1	Software
3.2	Equipment
3.3	Test Materials
3.4	Deliverable Materials
3.5	Proprietary Data
4	TEST SPECIFICATION
4.1	Requirements
4.2	Hardware Configuration and Design
4.3	Software System Functions
4.4	Test Case Design
4.4.1	Hardware Qualitative Examination Design
4.4.2	Hardware Environmental Test Case Design
4.4.3	Software Module Test Case Design and Data
4.4.4	Software Functional Test Case Design and Data
4.4.5	System-level Test Case Design
5	TEST DATA
5.1	Data Recording
5.2	Test Data Criteria
5.3	Test Data Reduction
6	TEST PROCEDURE AND CONDITIONS
6.1	Facility Requirements
6.2	Test Set-up
6.3	Test Sequence
6.4	Test Operations Procedures

Appendix I

Qualification Test Report

Appendix I

Qualification Test Report

This Appendix contains a recommended outline for the Qualification Test Report to be prepared by the test agency. The test report shall be organized so as to facilitate the presentation of conclusions and recommendations regarding software and hardware acceptability, a summary of the test operations, a summary of the test results, the test data records, and the analyses that support the conclusions and recommendations.

I.1 Introduction

The test agency shall identify and provide a brief description of the hardware and software that was tested, and any special considerations that affect the conclusions derived from the test results.

I.1.1 References

The test agency shall provide a list of all documents that contain material used in preparing the test report. This list shall include specific reference to applicable portions of the *Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems*, and to the vendor's Hardware and Software Specifications.

I.1.2 Terms and Abbreviations

The test agency shall provide a list and definition of all terms and nomenclature peculiar to the hardware, the software, or the test report.

I.2 Conclusions and Recommendations

The test authority shall list its conclusions regarding the degree to which the hardware and software meet the vendor's specifications and the standards. A list of conclusions regarding the acceptability of the vendor's technical and user documentation also shall be included.

Recommendations as to acceptability of the hardware and software shall be presented. These recommendations shall be based on the performance of the system software and the system hardware and source code inspection.

Any deficiency that remains uncorrected after completion of the qualification test and that has caused or is judged to be capable of causing the loss or corruption of voting data shall be described in detail sufficient to support a recommendation to reject the hardware or software being tested. Similarly, any deficiency in compliance with the security, accuracy, data retention, and audit requirements of Sections 2.3, 4.8, and 5 shall be fully described.

Any uncorrected deficiency that does not involve the loss or corruption of voting data shall not necessarily be cause for rejection. Deficiencies of this type may include failure to fully achieve the levels of performance specified in Sections 3, 4, and 6 of this standard. The nature of the deficiency shall be described in detail sufficient to support the recommendation either to accept or to reject the system, and the recommendation shall be based on consideration of the probable effect of the deficiency on safe and efficient system operation during all phases of election use.

I.3 Test Operations

The test authority shall provide a summary of the test, in sufficient detail to enable the understanding of the conclusions and recommendations, and of the description of test results, contained in the following section.

I.4 Test Results

The test authority shall summarize the test results. It is recommended that this synopsis be organized so as to facilitate comparison with the Qualification Test Plan. Summaries of hardware examinations, operating and non-operating hardware tests, software module tests, software function tests, and system-level tests shall be presented. The discussion of each group of tests shall contain specific test results which highlight the conclusions and recommendations. In addition, the ITA shall detail analyses and comments on the construction and correctness of the software code review.

I.5 Test Data Analysis

The test authority shall provide summary records of the test data and the details of the analysis. The analysis shall include a comparison of the vendor's Hardware and Software Specifications to the test data, together with any mathematical or statistical procedure used for data reduction and processing.

I.6 Appendices

The test authority shall provide other information relevant to the evaluation of the system as Appendices to the Qualification Test Report (e.g., documentation of the Physical and Functional Configuration Audits).

Appendix J

Acceptance Test Guidelines for P&M Voting Systems

Appendix J

Acceptance Test Guidelines for P&M Voting Systems

J.1 Introduction

Some general test criteria can be set forth to indicate the magnitude of performance testing required of P&M central and precinct count devices. The advisory sample sizes shown in the following tables are consistent with the demonstration requirements contained in the section on qualification testing, although they have been modified to produce statistical approximations for acceptance purposes.

J.2 Precinct Count System Criteria and General Procedures

As a guide, the following criteria apply to precinct count P&M systems:

- The number of ballots cast per device should be at least equal to the number of voters expected to use each device (500 to 750). It is preferred that the number be at least three times the maximum number of voters expected to vote on one device in any election held in the jurisdiction.

- The total number of contests per ballot should be at least 10, and at least thirty percent of the test formats should contain the greatest number of contests expected to occur in the jurisdiction.

- At least ninety percent of each ballot should be fully voted, and under- and overvotes should be randomly distributed across the ballots.

For the precinct count systems, it is assumed that there are 500 to 750 voters per device.

The following general procedures should be performed:

- open polls
- simulate primary election
- simulate general election
- cast 700 to 2000 test ballots
- close polls

- validate device report
- validate consolidated polling place report

J.3 Central Count System Criteria and General Procedures

As a guide, the following criteria apply to central count systems:

- The total number of ballots cast in simulated elections preferably should be equal to the maximum number of ballots expected in the largest election.

- For testing punchcard absentee ballot processing, the total number of test absentee ballots should equal at least 20 percent of the maximum number of registered voters in the jurisdiction.

- The total number of contests per ballot should be at least 10, and at least 30 percent of the test ballot formats should contain the greatest number of contests expected to occur in the jurisdiction.

- At least 90 percent of each ballot should be fully voted, and under- and overvotes should be randomly distributed across the ballots.

- The total number of ballots should be equally distributed among the actual number of card readers used.

The following general procedures should be performed:

- simulate primary election
- simulate general election
- cast 100 percent of expected number of ballots, simultaneously using all card readers
- validate precinct reports
- validate consolidated reports

EXHIBIT J-1

Suggested Ballot Quantities and Sample Sizes for
Performance Tests of Punchcard and Marksense
Voting Systems

Precinct Count

The total number of precinct devices to be subjected to performance test is computed as:

$$N = 50(\log(P)),$$

where N = number of units under test,
log = logarithm to base 10 and
P = number of polling places, greater than or equal to 100, with the restriction that 100 percent sampling shall apply to all cases where P is less than 100.

Assumptions:

- 30 cards (ballots) per minute
- average turn-out of 750 votes per precinct
- performance test sample size = 50 log(P)

Number of Precincts	Sample Size (Devices)	Number Ballots	Number Marks[1]
100	100	75,000	7,500,000
300	124	93,000	9,300,000
600	140	105,000	10,500,000
1200	155	116,000	11,625,000
2500	170	128,000	12,750,000
5000	185	138,000	13,875,000

1/ An average of 100 votes per ballot is suggested. For ease in preparing test data ballots, one could design a test with 10 contests, with each contest having 10 candidates, and vote for 10.

EXHIBIT J-1
(continued)

Central Count

Assumptions:

- 1500 registered voters per precinct
- average turn-out of 750 voters per precinct
- 100 precincts per device
- performance test sample size = 100 percent

Number of Precincts	Number of Systems[3]	Number Ballots	Number Marks[2]
100	2	75,000	7,000,000
300	3	93,000	9,300,000
600	6	105,000	10,500,000
1200	12	116,000	11,625,000
2500	25	128,000	12,750,000
5000	50	138,000	13,875,000

2/ Ibid.

3/ Includes all card readers or other data entry hardware.

Appendix K

Votomatic Ballot Cards Specifications

Appendix K

Votomatic Ballot Cards Specifications

K.1 Introduction

The most important specifications that apply to Votomatic ballot cards are those which insure that the cards are accurately and reliably read by the card readers on which they will be counted. System vendors typically specify card attributes which are essential for proper card handling and interpretation with their systems. In the event that a jurisdiction chooses to obtain card stock and print ballot cards according to other standards, the following specifications applicable to conventional data processing cards are provided.

K.2 Card Stock

Important characteristics of ballot card stock, and the standard test method used to verify compliance, are in the table below.

Table K-1

Ballot Card Stock Characteristics and Related Test Procedures

Specification	Test Procedure (1)
Composition: Stock shall be 100 percent chemical wood fiber; no ground wood allowed.	TAPPI T 401 m-60
Grain: The grain of the paper shall be in the direction of card length.	

Table K-1

Ballot Card Stock Characteristics
and
Related Test Procedures
(continued)

Specification	Test Procedure (1)
Defects: The paper shall be free of holes, wrinkles, loose dust, fuzz, abrasive materials, residual chemicals, static charges, slime spots and other brittle areas.	
Finish: The finish shall be without mottle and shall be uniform on both sides.	
Card Edge: a. Condition. All edges shall be smooth and free from burrs. b. Straightness. All edges shall fall between two straight, parallel lines .003 inch apart. c. Parallelism. Opposite edges shall be parallel within .003 inch. d. Squareness. All angles formed by adjacent sides shall be 90 degrees ± 5 minutes (.0047 at 3.2500 inches).	
Moisture Content: 4.5 to 6.5 percent of original weight (Test made on rolls at time of conversion).	TAPPI T 412 m
Electrical Resistance: 40 to 200 megohms.	IBM-9-01-0219
Basis Weight: 99 pounds ± 5 percent per ream of 500 sheets, 24" to 36".	TAPPI T 410 os-61
Thickness: 0/0070 inch ± 0.00004 inch.	TAPPI T 469 m-60
Burst Strength: 55 psi minimum.	TAPPI T 403 ts-63

Table K-1

Ballot Card Stock Characteristics
and
Related Test Procedures
(continued)

Specification	Test Procedure (1)
Stiffness: Either but not necessarily both of the following: With-grain / Cross-grain a. Taber 17.0 g-cm (min) 8.0 g-cm (min) b. Gurley 1200 mg (min) 500 mg (min)	TAPPI T 469 m-50
Folding Endurance (MIT): Minimum of 100 Double folds in each direction.	TAPPI 423 m-50 Method II
Folding Endurance (after aging): 25 percent maximum reduction in machine direction.	
Internal Tearing Resistance (Elmendorf): Minimum of 125 grams in each direction.	TAPPI T 414 ts-65
Ash: 2.0 percent maximum.	TAPPI T 413 ts-66
Hydrogen Ion Concentration: The Ph shall not be below 5.0.	TAPPI T 435 m-52 (Hot extraction)
Frictional Characteristics: a. Static coefficient of friction shall be between 0.30 and 0.45. b. Kinetic coefficient of friction shall not be less than 75% of the static coefficient of friction.	IBM 9-01-0213(3)
Expansion and Contraction: With 20% to 75% and 75% to 20% change in relative humidity. With-grain 0.25 percent max. / Cross-grain 0.70 percent max.	(4)

Table K-1

Ballot Card Stock Characteristics
and
Related Test Procedures
(continued)

Specification	Test Procedure (1)
Writing Quality: The paper shall be suitable for writing with pen and ink.	IBM 9-01-0210
Smoothness (Roughness): Average roughness on each side of the paper shall meet one, but not necessarily both of:	TAPPI RC-285 IBM 9-01-0209 TAPPI T 479 sm-48
a. Sheffield: no more than 125 Sheffields.	
b. Bekk: not less than 40 seconds and no more than 100 seconds.	
Abrasion Loss: The loss of weight from each side of the paper shall not exceed 50 milligrams.	IBM 9-01-0218 (5)
Air Resistance (Gurley): 95% of test units must fall within 35 to 140 seconds, and the remaining 5% must not exceed 160 seconds.	TAPPI T 460 m
Curl of Cards (20% rh and 75% rh): Types of curl for 3 1/4 inch by 7 3/8 inch specimen. Not less than 90% of samples shall meet the specification values, and no sample shall exceed a maximum value.	IBM 9-01-0216

	Specification	Maximum
Top-to-bottom	0.10 inch	0.12 inch
End-to-end	0.20	0.25
Diagonal	0.20	0.25

Table K-1

Ballot Card Stock Characteristics
and
Related Test Procedures
(continued)

NOTES:

1. Unless otherwise specified, all tests shall be performed on cards conditioned at 50 percent relative humidity and 73 degrees Fahrenheit by TAPPI (Technical Association of the Pulp and Paper Industry) Method T 402 m-49. Unless otherwise specified, relative humidity shall be controlled within ± 2 percent, and temperature within ± 3.5 degrees Fahrenheit.

2. Gurley stiffness shall be determined by the Gurley method given by the manufacturer of the testing equipment, using 2 x 2 1/2 inch specimens.

3. The instrument for performing the test of frictional characteristics shall consist of a smooth, level, metal plate to support the cards, a 3 x 3 inch 1,000 gram weight, a 1,000 gram capacity Chattilon push-pull gauge calibrated for horizontal use, and a motor-driven mount for the gauge which can advance the gauge horizontally and steadily at the rate of 3 feet per minute. The bottom of the weight shall have a smooth, clean rubber surface.

   In performing the test, eleven properly conditioned cards, which have been handled by their edges only, are laid flat on the metal plate with the left end of the cards against a stop. The top card is advanced to the right about 2 inches and the weight is placed on the cards, near the right end, so that it is supported by all cards. The gauge is then advanced toward the left so that it pushes against the weight in the direction of the long axis of the cards. A reading is taken when the weight and the top card move. This reading, in grams, divided by 1,000 is the status coefficient of friction. Ten successive read- ings are taken by sequentially placing the top card on the bottom of the deck and repeating the procedure. If, as the movement of the weight and top card continues, there is a change in the reading, the new reading, in grams, divided by 1,000 is the kinetic coefficient of friction.

4. Expansion and contraction tests are made by exposing cards sequentially to 20 percent, 75 percent, and 20 percent relative humidity at 73 degrees Fahrenheit. These cards shall remain fully exposed for a minimum of two hours at each humidity level. The cards are then measured with a precision of ± 0.0005 inch. The percent expansion is calculated from the difference between the original measurement at 20 percent relative humidity and that made at 75 percent. The

Table K-1

Ballot Card Stock Characteristics
and
Related Test Procedures
(continued)

percent contraction is calculated from the difference between the measurement at 75 percent relative humidity and the final measurement at 20 percent. If the relative humidity, as measured with a wet and dry bulb psychrometer, is not exactly 20 percent and 75 percent, but within the specified tolerance, corrections are applied assuming a straight line relationship between relative humidity and card dimensions.

5. Abrasion loss shall be determined by method TAPPI T 476 ts-63, Procedure 1, Dry Abrasion Test, except that the turntable of the abrading instrument shall make exactly 100 revolutions.

Table K-2

Ballot Card Dimensions:
228 Voting Positions

Description	Inches
General	
Distance, processable portion of card, bottom of card to perforation	7.375 ± .005
Card width	3.250 + .007 -.003
Locator Hole Locations and Dimensions	
Distance, bottom of card to bottom of hole.	10.155 ± .002 .005
Height of hole.	.315 ± .003
Width of hole.	.190 ± .002
Radius of curve at top and bottom of hole.	.095 ± .001
Distance, left edge of card to left edge of leftmost hole.	.280 ± .005
Distance, on centers, between holes.	2.125 ± .005
Distance, left edge of card to left edge of rightmost hole.	2.405 ± .010
End Stub with locator holes (perforation to top of hole).	3.375 ± .005

Table K-2

Ballot Card Dimensions:
228 Voting Positions
(continued)

Description	Inches
Pre-slit Hole Locations and Dimensions	
Height of pre-slit hole (chad length)	.125 ± .003
Width of pre-slit hole (chad width)	.070 ± .007 -.003
Left edge of pre-slit holes in left row to left edge of pre-slit holes in last row on right	2.750 ± .005
11 spaces between left edge and right edge at .250 inches, may vary ± .005 measuring from left edge to left edge of pre-slit holes	.250 ± .005
Distance from left edge of card to edge of first row of pre-slit holes	.188 + .007 -.003
Distance from bottom of card to bottom of edge of pre-slit in rows 12, 2, 6	.651 ± .007
Distance from bottom of card to bottom of edge of pre-slits in rows 11, 3, 7	.564 ± .007
Distance from bottom of card to bottom of edge of pre-slits in rows 1, 5, 9	.738 ± .007
Distance from bottom of card to bottom of edge of pre-slits in rows 0, 4, 8	.825 ± .007
Corner Cuts	
Corner cut—left edge	.250 ± .016
Corner cut—left bottom portion	.433 ± .016

Table K-2

Ballot Card Dimensions:
235 Voting Positions

Description	Inches
General	
Distance, processable portion of card, bottom of card to perforation	7.375 ± .005
Card width	3.250 + .007 -.003
Locator Hole Locations and Dimensions	
Distance, bottom of card to bottom of hole.	10.155 ± .002 .005
Height of hole.	.315 ± .003
Width of hole.	.190 ± .002
Radius of curve at top and bottom of hole.	.095 ± .001
Distance, left edge of card to left edge of leftmost hole.	.270 ± .005
Distance, on centers, between holes.	2.125 ± .005
Distance, left edge of card to left edge of rightmost hole.	2.395 ± .010
End Stub with locator holes (perforation to top of locator hole).	3.375 ± .005

Table K-2

Ballot Card Dimensions:
235 Voting Positions
(continued)

Description	Inches
Pre-slit Hole Locations and Dimensions	
Height of pre-slit hole (chad length)	.125 ± .003
Width of pre-slit hole (chad width)	.070 + .007 -.003
Left edge of pre-slit holes in left row to left edge of pre-slit holes in last row on right	2.750 ± .005
11 spaces between left edge and right edge at .250 inches, may vary ± .005 measuring from left edge to left edge of pre-slit holes	.250 ± .005
Distance from left edge of card to edge of pre-slit holes	.188 + .007 -.003
Distance from bottom of card to bottom edge of pre-slit holes in rows 12, 3, 5, 6, 7, 8, 9	.477 ± .007
Distance from bottom of card to bottom edge of pre-slit holes in rows 11 and 2	.651 ± .007
Distance from bottom of card to bottom edge of pre-slit hole in row one (1)	.564 ± .007
Distance from bottom of card to bottom of pre-slit hole in rows 0 and 4	.738 ± .007
Corner Cuts	
Corner cut—left edge	.250 ± .016
Corner cut—left bottom portion	.433 ± .016

Table K-2

Ballot Card Dimensions:
312 Voting Positions

Description	Inches
General	
Distance, processable portion of card, bottom of card to perforation	7.375 ± .005
Card width	3.250 + .007 -.003
Locator Hole Locations and Dimensions	
Distance, bottom of card to bottom of hole.	10.112 ± .002 .005
Height of hole.	.315 ± .003
Width of hole.	.190 ± .002
Radius of curve at top and bottom of hole.	.095 ± .001
Distance, left edge of card to left edge of leftmost hole.	.280 ± .005
Distance, on centers, between holes.	2.125 ± .005
Distance, left edge of card to left edge of rightmost hole.	2.405 ± .010
End Stub with locator holes (perforation to top of locator hole).	3.375 ± .005

Table K-2

Ballot Card Dimensions:
312 Voting Positions
(continued)

Description	Inches
Pre-slit Hole Locations and Dimensions	
Height of pre-slit hole (chad length)	.125 ± .003
Width of pre-slit hole (chad width)	.070 + .007 -.003
Left edge of pre-slit holes in left row to left edge of pre-slit holes in last row on right	2.750 ± .005
11 spaces between left edge and right edge at .250 inches, may vary ± .005 measuring from left edge to left edge of pre-slit holes	.250 ± .005
Distance from left edge of card to edge of first row of pre-slit holes	.188 + .007 -.003
Distance from bottom of card to bottom of edge of pre-slits in all 12 rows	.564 ± .007
Distance from bottom edge of pre-slit hole in bottom column to bottom edge of pre-slit hole in top column	6.525 ± .007
Corner Cuts	
Corner cut—left edge	.250 ± .016
Corner cut—left bottom portion	.433 ± .016

Appendix L

Glossary

Appendix L

Glossary

Acceptance Test—The examination of voting systems and their components by the purchasing election authority in a simulated use environment to validate performance of delivered units in accordance with procurement requirements; testing to validate performance may be less broad than that involved with qualification testing and successful performance for multiple units (precinct count systems) may be inferred from a sample test.

Adoption Date—The date upon which the state adopts the standards.

Algorithm—A prescribed set of rules, processes, or sequence of steps (often iterative) to be followed to arrive at the solution to a problem.

ASCII (American Standard Code for Information Inter-change)—A standard 7-bit 96-character code used to exchange information among equipment units of different manufacture, such as a computer and its peripherals. It is also the standard for digital communications over telephone lines.

Assembler—A program that translates assembly language source code into machine-language object code. Each assembly language instruction is translated into one corresponding machine-language instruction. After all translation has taken place, the program is ready for execution by the computer.

Assembly Language—A lower level computer language which uses mnemonic instructions. It gives the programmer control over machine operations, and can manipulate data at the byte level, and, on some systems, at the bit level.

Audit Trail—The continuous trail of evidence linking individual transactions related to the vote count with the summary record of vote totals. It permits verification of the accuracy of the count and detection and correction of problems. A combination of manual and computer-generated documentation provides a record of each step taken in: defining and producing ballots and generating related software for specific elections; installing ballots and software; testing system readiness; casting and tabulating ballots; and producing reports of vote totals. The record incorporates system status and error messages generated during election processing, including a log of machine activities and routine and

unusual intervention by authorized and unauthorized individuals. Also part of an election audit trail, but not covered in the technical standards, is the documentation of such items as ballots delivered and collected, administrative procedures for system security, pre-election testing of voting systems, and maintenance performed on voting equipment.

Ballot Image—A corresponding representation in electronic form of the punch, mark, or vote position of a ballot.

Baseline—A software configuration at the time of submittal for testing against the Voting System Standards. Future configurations of the software shall be identified in terms of the baseline and the approved changes thereto.

Bit Error Rate—The number of errors divided by the total bits that are processed; the gauge of system accuracy.

Block—An element of structure for program coding which consists of declarations of data objects and their types, a BEGIN statement, descriptive comments, a sequence of statements that describe operations to be performed on the data objects listed in the declarations, and an END statement.

Branch—To depart from the sequential execution of the statements in a program by command. A branch may be conditional or unconditional. A conditional branch is one in which the flow of the program is altered from executing the next sequential instruction if certain conditions are met. An unconditional branch is one in which the flow of the program is always directed to some statement other than the next statement in the sequence of the program regardless of the condition.

Card Reader—A necessary peripheral device for computers, used to read the data from punch card ballots.

Catastrophic System Failure—A total loss of function or functions as opposed to a partial loss or degradation of function, such as, the loss or unrecoverable corruption of voting data, or the failure of an on-board battery for volatile memory.

Central Processing Unit (CPU)—The CPU performs all the arithmetic and logic operations, and controls the flow of information throughout the entire computer system.

Certification Testing—The state examination, and possibly testing, of a voting system to determine its compliance with state counting law and rules and any other state requirements for voting systems.

Checkpointing—A recovery method by which the system is designed to save all information necessary to define the state of the system at some point in time.

Circuit—A system of conducting paths and the electronic elements they connect that is constructed to perform a specific function.

Code—As a noun, code means the system of characters, symbols, logic relationships, and rules for representing information. As a verb, to code means the same as to write, as in to code a program.

Compiler—A program that translates a source program written in a higher level language such as COBOL or FORTRAN into a machine language program, written in object code that a computer can execute. A compiler may generate more than one machine language instruction for each source code instruction, whereas an assembler generates only one machine language instruction for each source code instruction. A compiler generates the complete object code program before it is executed by the computer.

Component—Independent item having a life of its own that is incorporated into the system, such as a card reader, printer, modem vote recorder as contrasted with smaller parts like a circuit board.

Computer Program—A collection of instructions coded according to specific rules, and in a specific sequence, that a computer can execute directly, or that can be translated into object code which the computer can execute. The program tells the computer what to do.

Data Accuracy—A term that refers to the system's ability to process voting data absent errors generated by the system internally. It is distinguished from data integrity which encompasses errors introduced by an outside source.

Data Base—The entire file or collection of data that is relevant to a particular application or the entire computer system, that is processed by the system over an extended period of time.

Data Integrity—A term that refers to the invulnerability of the system to accidental intervention or deliberate, fraudulent manipulation that would result in errors in the processing of voting data. It is distinguished from data accuracy which encompasses internal, system generated errors.

Data Security—The various methods and procedures, such as the use of passwords and encryption, implemented to prevent unauthorized use, destruction, or disclosure of data, whether it is accidental or deliberate.

Diagnostic Program—A test program used to test the individual units of a computer system, or the entire system itself, when the user suspects a hardware or software malfunction. Diagnostic programs can be used to test memory, the instruction set, and the various peripheral devices in an attempt to pinpoint the cause of a specific problem.

Documentation—Facts, notes, or instructions which are used to explain system functionality, software and hardware characteristics, and developmental testing. Many programming languages allow for documentation within the program itself.

Driver—A program or subprogram designed to control the operation of a specific piece of peripheral hardware, such as a card reader, printer or disk drive. The driver takes into account the specific characteristics unique to the device.

Effective Date—The state determined date after which systems presented for certification or acquisition should be in adherence with the standards.

EEPROM (Electrically Erasable Programmable Read-Only Memory)—Generally, read-only memory is memory which is nonvolatile and cannot be erased. An EEPROM is nonvolatile (will hold its data if power is shut off to it) but can be erased through a technique of pulsed signals.

Escrow—Third-party custody, for safekeeping and possible verification, voting system software (source code), including all updates, modifications, or new versions.

Examination or Review—The inspection or analysis by a test authority, state certification authority, or local jurisdiction of the system hardware, software and other system documentation, test documentation, or documentation of modifications to ascertain if the system complies with the standards, state code, or procurement contract requirements and to determine if further testing is required.

Existing Systems—Computerized voting systems that were not originally designed to be in compliance with the standards, most of which are currently in use and all of which will have been marketed or, if developed in-house, used prior to the effective date of the standards set by the states.

FEC—An acronym for the Federal Election Commission.

Firmware—Computer programs (software) stored in read-only memory (ROM) devices imbedded in the system and not capable of being altered during system operation.

Flowchart—A symbolic representation of the sequence of steps and the associated logic of a computer program. A flowchart is usually drawn before a programmer begins to code a program, to assist in visualizing the flow of the program. There is a standard set of flowchart symbols.

Full Compliance Date—A date on which all systems in use in the state would be in total compliance with the performance and design standards, i.e.; the point at which all existing systems would no longer be grandfathered.

Functional Test—A test performed to verify or validate the accomplishment of a function or a series of functions.

Hardware—The mechanical, electrical and electronic assemblies, including materials and supplies, which are a part of the system, such as microprocessor, disk drives, printer, circuit boards, integrated circuits.

Higher Level Language—A language which allows the programmer to write in a notation which is familiar, such as the use of English language words, as opposed to writing in mnemonics or directly in object code. Examples of higher level languages are BASIC, COBOL, FORTRAN, and Pascal. Generally, higher level languages are easier to learn, and the programmer is less apt to make mistakes, than lower level languages such as assembly language. A higher level language must be translated into object code by a compiler or interpreter.

In-house Systems—Computerized voting systems usually composed of commercial hardware and specially tailored software. In most instances, the tally software initially has been procured from a third party, then tailored or enhanced to meet the special needs of the jurisdiction by in-house data processing personnel, or outside software consultants hired by the local jurisdiction.

Initialization—To return a computer to its original state when a program was first run by returning all counters, i.e., memory, to zero or their starting values.

Input/Output Devices—Those peripheral devices that allow human interface, storage of data, hard copy, or communication with another computer, such as keyboards, disk drives, printers, and modems.

Integrated Circuit—A microcircuit with all necessary components fabricated on a single chip. The chip is mounted inside a package, with pins along the side, that allows it to be plugged into a socket, or soldered directly onto a circuit board. The entire package is often referred to as the integrated circuit.

ITA—An acronym for independent test authority.

Light Pen—A hand-held, pen-shaped, photosensitive device allowing a user to select, draw, or modify information on a CRT. The CPU can determine the coordinates of the light pen when it is touched to the screen. Light pens are very valuable in CAI or CAD applications, because the user does not have to be aware of the internal program that controls it in order to use it.

Logical Correctness—A condition signifying that, for a given input, a computer program will satisfy the program specification (produce the required output).

Loop—A portion of a computer program repeated a given number of times, or until a certain result is obtained. A loop may contain only a few instructions or several hundred.

Lower Level Language—A computer language in which the instructions usually bear a one-to-one relationship with object code or machine language. Lower level languages are difficult to code in because they require a great amount of coding to perform simple tasks, and bear no resemblance to the English language, as many high-level languages do. Assembly language is a lower level language.

Machine Language—Machine language is the lowest level of programming, in which all instructions and data are represented in binary form. Programming directly in machine language consists of supplying the microprocessor in binary form with machine instructions, memory locations, and data in certain sequences. The program helps the microprocessor distinguish between instructions and data.

Mainframe—A generic term referring to the earlier large computers that rely primarily on punched cards for their input. Basically, any computer which is not a minicomputer or a microcomputer is a mainframe.

Marksense Voting System—A system by which votes are recorded by means of marks made in voting response fields designated on one or both faces of a ballot card or series of cards.

Memory—Any device in a computer system where information can be stored for future use. The internal memory of a computer consists of ROM and RAM. ROM is Read-Only Memory. It is nonvolatile in that its contents remain stored even if power is removed. Information can be read from ROM, but cannot be placed into ROM. RAM is volatile memory. The contents of RAM will be destroyed if power is removed, and can be written over by the user. RAM is used to store the programs and information that the computer is currently processing.

Microprocessor—A chip that is the central processing unit of a computer containing the arithmetic-logic unit, a control unit, and data registers. Each microprocessor has its own unique instruction set.

Modified Existing Systems—Existing systems that have been modified to be in partial or full compliance with the performance and design standards.

Modified New Systems—Voting systems previously developed tested in compliance with the standards and that are subsequently modified.

Modular Design—A method of software design in which an independent body of code statements performs a single logical function. The module is self-contained, and its removal from the program will disable only its unique function.

Monitor—A computer program that detects, interprets,and executes a function designated by closure of a switch or by keyboard input. An operating system is a more elaborate program (including a monitor) that also performs or controls other system functions.

Network—An interconnected system of transmission lines that allows computers, terminals, peripheral devices, and similar types of equipment to communicate with each other.

New Systems—Computerized voting systems that have been designed and tested in compliance with the performance, design, and test standards, and that are first marketed or, if developed in-house, first used in the future (i.e.; 1990 or later).

Nonvolatile Memory—Memory in which information can be stored indefinitely with no power applied. ROMs and EPROMs are examples of nonvolatile memory.

Object Code—The binary code produced by a compiler or assembler that can be executed directly by a computer without further simplification. A machine language program is written in object code.

Operating System—A supervisory program or collection of programs, used to manage the hardware and logic functions of a computer. An operating system may perform debugging, control the I/O devices, run the compiler or interpreter, and perform a variety of other housekeeping chores.

Parity Check—A method of determining the validity of data in which the summation of the binary digits for each work, or other specified piece of data, is checked against a previously computed parity digit.

Password—A word, string of characters, or sequence of numbers which allows the user or the computer to access protected information. For example, a computer needs the appropriate password to access disk storage.

Peripheral Devices—Hardware that is external to the microprocessor in a computer. For example, the CRT, keyboard, printer, and disk drives are considered peripheral devices, even if they are housed within the same cabinet as the microprocessor. Data communications devices, such as modems, are also considered peripheral devices.

Printed Circuit—A circuit in which conducting strips are printed or etched into an insulating board, and used in place of wires, to form the conductive path between the various circuit components.

Programming Language—A systematic and structured means of communicating with a computer through the use of a defined set of characters written in predetermined sequences. There are three levels of programming languages. Machine language, which consists of binary object code, is the lowest level. Next come low-level languages, such as assembly language, which uses mnemonics as aids for the programmer. Low-level language instructions are usually translated on a one-to-one basis into object code. FORTRAN, BASIC, COBOL, and Pascal are examples of higher level languages. They contain familiar English words, and must be translated into object code through the use of a compiler or interpreter. There are usually many machine language instructions for each source code instruction written in a higher level language.

PROM (Programmable Read-Only Memory)—A nonvolatile, or permanent, memory which can be programmed by the device manufacturer or supplier.

Protocol—The specific sequence of signals in the initial exchange between two communications devices, to make sure that the two devices can recognize each other's signals, and that the information being transmitted and received is intelligible. A protocol determines what pattern the flow of data bits will follow, and how the devices will cooperate in their communication. Protocols can be used between a computer and its peripherals. Protocols are common in networks, to verify that the user has authority to use the network.

Punchcard Voting System—One where votes are recorded by means of punches made in voting response fields designated on one or both faces of a ballot card or series of cards.

Qualification Testing—The examination and testing of a computerized voting system by an independent test authority using FEC test standards to determine if the system complies with the FEC performance and design standards. This process would occur prior to state certification.

RAM (Random Access Memory)—Memory that provides immediate access to any information in storage. RAM in computers is in the form of an integrated circuit, that provides the computer with quick-access volatile memory. Information can be read from or written to RAM. However, when the power is turned off, all information in RAM is lost.

Random Number—A number selected from a group of numbers in such a way that each number in the group is equally likely to be chosen. Most programming languages for computers have the ability to select random numbers.

Recertification—The state examination, and possibly the retesting, of a voting system which was modified subsequent to receiving state certification. The object of this process is to determine if the modification still permits the system to function in accordance with state requirements.

Remote Device—A peripheral device that is not on-site, and is connected to a computer by a communications link, such as a telephone line, through the use of a modem or similar device.

ROM (Read Only Memory)—A nonvolatile form of memory that, once programmed, cannot be changed. ROM can be read from, but cannot be written to. If power is lost, the information in ROM remains. Also, the information in ROM cannot be changed by a computer operation.

Software—The application and operating system programs associated with a computer, as opposed to hardware that refers to the physical components of a computer system.

Source Code—A programmer codes a program in a specific language called source code. The source code of the computer language is then compiled, interpreted, or assembled into object code by the computer. The result is a machine language program in binary form which can be run by the computer.

Subroutine—A set of programming statements or instructions that perform a specific task. A subroutine may be jumped (or branched) to, from any part of the master program. The last statement in the subroutine returns the logic of the program back to the point from which it originated. A subroutine is created when the need arises for a certain type of calculation or processing at various points in a master program. Instead of repeating the steps at each of the points, they are put in a subroutine, that can be called at each of the points with a single statement.

Subsystem—A group of component or a single piece of equipment which performs a unique or identifiable function.

Systems Software—The software for a particular computer, supplied by the manufacturer, and necessary for the basic operation of the system. The software may be resident in ROM, or provided on disk or tape. Systems software generally includes the operating system, the I/O routines, diagnostic and debugging programs, and the programming language capabilities.

Table-driven Program—A computer program designed such that all the parameters that distinguish a particular execution of the program from any other execution may be found in a set of tables contained in the program.

Unconditional Branch—A statement that interrupts the normal process of executing instructions in the sequence, and specifies the next instruction to be executed.

Utility—Computer software or firmware of a generic nature that assists the computer (and the programmer) in performing tasks as directed in specific applications programs.

Validation—A test to find errors by executing a program in a real environment, i.e., during acceptance tests.

Verification—A test to find errors by executing a program in a simulated environment, i.e., during system qualification.