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.

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 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 reopening 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.

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.

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 systemlevel 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 processsing 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 l 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 nonoperation 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. 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.

3.4.1.1 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). 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
- 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.

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.

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 mainte-nance 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 noncritical 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:

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

Machine 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 readwrite-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 500137, 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. 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); 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	A,B corner, total of 26
Movable	Twice on each bottom	A,C edge and corner, total of 16
Fixed	On each bottom corner	A,C and edge, total of 8

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 MILSTD-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 10Remove 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 11Inspect 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 10Repeat Steps 5 through 8, with temperature at the high operating limit, complete at T=24 hrs.

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

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

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

Step 14Reconnect 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;

©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 opera-

tions;

(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;

©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.

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.

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)

©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)

©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.

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 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.

•

A PLAN FOR IMPLEMENTING THE FEC VOTING SYSTEM STANDARDS

FEDERAL ELECTION COMMISSION
JANUARY 1990

APRIL 1990 REVISIONS TO THE IMPLEMENTATION PLAN

Section 6

A paragraph was added to Subsection 6.5 to clarify that the escrow plan is not intended to preclude release of deposited materials to a criminal investigative tribunal or upon court order in a criminal proceeding.

Section 7

The second indented paragraph in Subsection 7.3 has been rewritten to clarify

that the independent test authority's original qualification test report should be sent directly to the escrow company as an update to the deposit. There, it would be separately available upon request. Copies of the report would be transmitted

to the vendor and to the Federal Election Commission.

The third paragraph in Subsection 7.7 has been rewritten to clarify the flow of information among the vendor, the escrow company, and the independent test authority when evaluating system modifications.

TABLE OF CONTENTS

A Plan for Implementing the FEC Voting Systems Standards

1.0 Introduction

In 1985, the Federal Election Commission (FEC) undertook a long-term, multi-faceted commitment to develop voluntary standards for computer-based voting equipment.

The product of this effort, Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems, contains minimum performance criteria for computerized hardware and software voting systems and the tests methods required to demonstrate adequate performance.

The FEC project to develop voting system standards was authorized by the U.S. Congress in response to calls for assistance from states confronted by voting system failures and increasingly complex voting system technology. In accordance with the Congressional mandate, the standards are voluntary. They may be adopted in whole or in part, or completely disregarded by the states. Furthermore, some states may choose to place stricter performance requirements on voting systems that will be used in their jurisdiction.

The technical standards and test criteria are accompanied by an escrow plan, an independent test authority evaluation plan, and this implementation plan. The System Escrow Plan for the Voting System Standards Program defines a means of controlling access to proprietary information, such as source code and system documentation, which may be needed by the user for system maintenance and which the voting system vendors must furnish for system testing. A Process for Evaluating Independent Test Authorities outlines procedures for ensuring that independent test authorities have adequate internal quality controls, facilities, equipment, and personnel with the appropriate knowledge and experience; and that no conflict of interest exists between these companies and any voting system vendor. Associated management guidelines will be provided in the future and will discuss several issues related to the standards including computer security, pre-election testing, voting system procurement, and system operations.

This Implementation Plan provides information and advisory guidelines to assist states in the implementation of the standards. Section 2.0, below, discusses the roles of and relationships among the seven participants involved in implementation (the Federal Election Commission, the National Voluntary Laboratory Accreditation

Program of the National Institute of Standards and Technology, the independent test authorities, the states, the local jurisdictions, the vendors, and the escrow agents). Section 3.0 identifies alternative state implementation strategies. Section 4.0 highlights issues states should consider when adopting and applying the standards to existing, modified and new systems. The process of evaluating independent test

authorities is summarized in Section 5.0. Section 6.0 outlines decisions that states must make with regard to the escrow of source code and other proprietary documentation. Section 7.0 describes the ideal flow of information among the seven participants involved in implementing the standards.

1.1 Preliminary Considerations

Before advancing into the details of this implementation plan there are a few items of a general nature which warrant consideration.

1.1.1 A Nationwide Implementation Strategy

The success of the standards program will depend, in large part on the extent to which states choose to employ the FEC standards. Once several large states adopt the FEC standards, any vendor seeking to market their product nationwide will likely have to embrace these requirements as part of their general offering. In this way, the market dominance of California, New York, and a handful of other states can lead to a nationwide impact of these standards even if many of the other states take no action at all.

Nevertheless, individual states will want to focus on the needs of their own jurisdiction and determine how best to implement performance and test standards. In doing so, states should be cautioned about adopting significantly stricter standards than the FEC standards that may impede the design and development of new, innovative equipment. State adopted standards also ought not force the vendors to price the voting systems out of the range of smaller local jurisdictions.

States should consider accepting as sufficient those national qualification tests performed by independent test authorities instead of requiring vendors to submit to a second general qualification test performed by a state designated test authority. States may also choose to recognize certification testing conducted by other states.

Such a policy would not, of course, preclude state certification testing for features specific to that state. If states coordinate their certification processes or at least avoid duplicating qualification tests performed by an independent authority and relevant tests performed by other states, they will minimize costs of implementing the standards in all jurisdictions.

1.1.2 Cost Implications

The projected costs of implementing the standards will not be inconsequential. The qualification tests, to be performed on a national level by independent test authorities,

will be expensive. Additional costs will be incurred if existing systems are upgraded. Although the voting system vendors may well absorb these costs initially, the expense will eventually be passed on to the user in the form of higher prices.

In recognition of these cost factors, and of state and local fiscal constraints, a few decisions were reached regarding the standards based on cost/benefit analyses. One example relates to testing. Instead of an exhaustive examination of software source code, the standards propose a selectively in-depth review. This decision was reached because the cost of the former could not be justified by its anticipated benefits, and because the documentation required of the vendor and a number of tests required by the standards should identify problem areas. Another example is the position that the standards were never intended to apply to existing systems to the extent that software would have to be entirely rewritten to adhere to the standards' requirements. Instead, resources might better be spent on collecting documentation on existing systems for use in testing and maintenance or, if necessary, replacing the software.

1.2 Definitions

Several terms used in this document warrant definition:

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.

Modified existing systems _ Existing systems that have been modified to be in partial or full compliance with the performance and design standards.

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).

Modified new systems _ Voting systems previously developed and tested in compliance with the standards that are subsequently modified.

In-house systems _ Computerized voting systems usually composed of commercial hardware and specially tailored software. In most instances, the tally software initially is 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.

Adoption date _ The date upon which the state adopts the standards.

Effective date _ The state determined date after which systems presented for certification or acquisition should be in compliance with the standards.

Full compliance date _ A date on which all systems in use in the state would be in compliance with the performance and design standards (i.e., the point at which all existing systems would no longer be grandfathered).

Examination or review _ The inspection or analysis by a test authority, state certification authority, or local jurisdiction of the system hardware, software and 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 what further testing is required.

Testing _ The physical and functional testing of a voting system.

National 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.

State certification testing _ The state examination, and possibly testing, of a voting system to determine its compliance with state vote counting law and rules and any other state requirements for voting systems.

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.

Local acceptance testing _ The examination and testing of voting systems and their component parts by the purchasing election authority in a simulated use environment to ensure delivered units perform in accordance with procurement requirements. Testing to validate performance may be less extensive than that conducted during qualification testing. Successful performance for multiple units (precinct count systems) may be inferred from a sample test.

ITA _ An acronym for independent test authority.

FEC _ An acronym for the Federal Election Commission.

NVLAP/NIST _ An acronym for the National Voluntary Laboratory Accreditation Program of the National Institute of Standards and Technology.

1.3 Topics Discussed in this Plan

The remaining sections of this implementation plan present the following topics for state consideration:

The recommended roles of the seven participants involved in the implementation of the standards;

The alternatives for state implementation of the standards including the recommended timing of, the possible approaches to, and the enabling vehicles for adoption;

The recommended application of the standards and testing requirements to existing, new and modified voting systems, including in-house systems;

The evaluation of independent test authorities;

The escrow of software source code and other vendor proprietary information; and

The flow of information among participants in the implementation of the standards.

2.0 Roles of the Participants

The successful implementation of the standards will require the combined efforts of different entities: the Federal Election Commission, the National Voluntary Laboratory Accreditation Program of the National Institute of Standards and Technology (NVLAP/NIST), the independent test authorities, the states, the local jurisdictions, the vendors, and the escrow agents. Following are brief summaries of their respective roles as they are currently envisioned.

2.1 The Role of the Federal Election Commission

The primary responsibility of the Federal Election Commission (FEC) will be to assist the other participants in implementing the standards. In this role, the FEC's National Clearinghouse on Election Administration (the FEC Clearinghouse) will serve as a central repository for many documents associated with the implementation process including: information regarding the evaluation of independent test authorities; copies of qualification, certification, and acceptance test plans and test reports (subject to strict control and propriety interests); data from independent test authorities, states, and vendor reports in order to track systems qualification, certification, and procurement nationally; and other such data and information as may prove generally useful.

The FEC will also be involved with NVLAP in setting criteria for vendors to use when evaluating independent test authorities.

2.2 The Role of NVLAP/NIST

NVLAP/NIST will assist the FEC the development of broad criteria that can be used by vendors to evaluate independent test authorities. However, until (and unless) a formal ITA accreditation program is established, NVLAP will not supervise the process or make the final determination to approve an ITA.

If funding to establish an accreditation program becomes available, a second phase of the evaluation process will be initiated. During this phase, NVLAP/NIST will have the primary responsibility for evaluating ITAs on a regular basis, using detailed accreditation protocols. Accredited test authorities will receive an accreditation certificate from NVLAP.

2.3 The Role of the Independent Testing Authority

Independent test authorities (ITAs) will conduct qualification tests on new systems (or substantially modified systems) supplied by vendors. They will also be responsible for determining whether or not a modification necessitates partial or complete system retest. ITAs will forward test results and modification determinations to the appropriate states and local jurisdictions as well as to the FEC Clearinghouse in order to ensure that other participants are aware of which systems have been qualified.

Independent test authorities may also be consulted by state or local election officials when planning and conducting state certification or local acceptance tests, respectively.

2.4 The Role of the States

The primary role of the states will be to adopt standards, determine when they will become effective, decide how to deal with existing systems, and perform appropriate certification tests on all systems intended for use within the state. The FEC recommends that states also keep records of all certified systems, monitor voting systems procured from vendors (along with any in-house developed or enhanced vote tallying systems), and transmit this information to the FEC. Finally, states will serve a key role in negotiating escrow agreements for systems that are used within their jurisdiction. The state may also choose to play a pivotal role in retaining ITA tested software and, upon installation, compiling and shipping only executable modules to local jurisdictions.

2.5 The Role of Local Jurisdictions

The primary function of local jurisdictions in the application of the standards will be to procure only those voting systems that comply with state standards, and perform acceptance tests as well as pre-election logic and accuracy tests on all voting equipment acquired. The FEC urges local jurisdictions to report to the state any system developed or modified in-house and any modifications procured from a vendor. And finally, local jurisdictions should enter into escrow agreements for systems procured and should also escrow in-house developed or enhanced software.

2.6 The Role of the Vendors

Vendors bear several responsibilities. They should, for example: if economically feasible, modify existing systems to meet the performance and design standards or, at least, incorporate the security and audit trail capabilities described in the standards; design all systems which will be first marketed in the future to at least comply with the minimum performance and design standards and have them qualified by an independent test authority; submit their systems (along with appropriate documentation) to examination or testing required by the states; deposit into escrow all source code and proprietary information for existing and new systems; and inform the FEC Clearinghouse of all qualified equipment and provide updated listings of the jurisdictions using each software version.

2.7 The Role of the Escrow Agents

Much like the FEC, the escrow agent will serve as a neutral entity serving both vendors and users. While interacting with state and local jurisdictions, the escrow agent will maintain the confidentiality of the vendor's proprietary information. The escrow agent will also keep records of which systems are in escrow and which local users sign on to master software deposits. The agent may also be required to verify software used by a particular jurisdiction against the archival version in escrow.

3.0 Alternative State Implementation Strategies

From the outset, states must decide if, when, how, and by what means they intend to adopt the FEC standards (as well as any other recommendations proposed by reputable sources). States which fall under the preclearance provisions of the Voting Rights Act must also take that into account when planning their approach.

3.1 Timing of Adoption

States should consider adopting the performance and test standards for voting systems as soon as they are released, rather than waiting for the companion management guidelines. Guidelines for voting system procurement, pre-election testing, computer security, and system operations will be available at a later date and may be adopted at that time. (A discussion of the state's role in these areas will be provided with the management guidelines.)

3.2 Transition Options

Standards for any commodity are not normally applied to products that are already in use. For example, the initial requirement for safety belts in automobiles did not affect those cars already manufactured. Likewise, requiring the immediate application of the voting system performance, design and testing standards would be unreasonable, unrealistic, and very costly. Modifying existing systems or developing and qualifying new ones involves both time and money. Furthermore, it is unlikely that older existing systems will be brought into compliance with some of the provisions of the standards such as full system documentation, modular and structured code, and complete audit trails.

The FEC also recognizes that states and local jurisdictions would suffer financial hardship and would have few new systems from which to choose if systems presently in use, but which do not meet the minimum standards, had to be summarily replaced. Therefore, existing voting systems are likely to continue in use for a while. Still, safeguarding the integrity of the vote counted by these systems is a legitimate concern.

In light of these considerations, the FEC proposes that states pursue a gradual implementation of the standards over a period of time. Vendors could continue to market their existing systems during this time, while working on modifications necessary to bring them into full or partial compliance with the standards. Users of in-house developed systems also could modify their systems. New systems meeting all minimum standards would also be developed and tested during this period. In addition, the FEC recommends that states adopt measures to promote the use of high level language in certain key portions of software programs developed in the future.

This recommendation is not intended to preclude the continued use of existing or soon to be released assembly language software that conforms to state requirements and

that has been shown to comply with the standards. (See Exhibit A for a recommended implementation timetable.)

3.2.1 Establishing an Effective Date

The FEC recommends a gradual implementation of the standards by targeting an effective date approximately two years subsequent to the adoption of the standards, after which only systems that are in compliance with the standards may be acquired. Up until that point systems that do not meet the minimum standards could be obtained. For example, states that adopt standards early in 1990 might establish January 1992 as the date beyond which newly acquired systems would have to be in compliance. States adopting the standards at a later time could shorten this interim period because new and modified existing systems would already be under development in response to the states that had adopted standards earlier.

States may deal with existing systems that continue to be used after this effective date by employing a full compliance target date, by simply exempting them from the application of the standards (i.e.; grandfathering them), or by requiring system modification or administrative procedures to provide minimum security and audit trail capability. Each course of action, as described below, has positive and negative aspects.

3.2.2 Employing a Full Compliance Date

If employing this provision, states would determine that existing computerized ballot tabulation systems should not be used beyond a certain date if they do not comply with the standards. This date should be well past the effective date of the standards. For example, states that adopt the standards in 1990 and set an effective date of 1992 might set a target date in 1996. Local jurisdictions would have to take one of the following actions under this provision:

Acquire modifications to their existing system to bring it into compliance.

This option would most likely involve the upgrade of software and system documentation and might not be practical for older systems (i.e.; those introduced more than five years before the formal release of the voluntary standards by the FEC); or

Replace their existing system with a new, qualified system or another existing system which has been modified to comply with the standards.

The advantage of this approach is that it would ensure a gradual, yet complete transition to systems which comply with the standards. The disadvantage is that it usually requires local jurisdictions to shoulder the financial burden of replacing or modifying their voting systems. The cost will be significantly higher for jurisdictions with older precinct count systems. Existing systems that have been recently introduced may, for the most part, be more easily modified to comply with the standards. Older systems, particularly those no longer marketed, will probably have to be replaced. Some older systems which incorporate commercial hardware, however, might only require replacement of the software.

3.2.3 Grandfathering Existing Systems

The adverse financial impact of replacing existing systems may be avoided if states choose to grandfather those in use as of the effective date of the standards. Nevertheless, this approach will permit the continued use of voting systems that have not been shown to meet minimum standards for adequate performance. Lack of proper security and audit trail capabilities and other problems associated with the use of these systems may well jaundice the public's view of the integrity of the election process and the effectiveness of the standards. Therefore, in order to ensure the accountability of these systems, the FEC urges states to recommend that local jurisdictions obtain copies of system user, operator, and maintenance manuals for these systems and: recommend that user jurisdictions upgrade/retrofit their system with all required audit trail items and security provisions; or mandate specific administrative procedures to be used in the event it is not feasible to upgrade/retrofit certain systems with security or audit trail capabilities.

In considering the options available, states will want to weigh the benefits of each measure (e.g.; long term cost savings of retaining, modifying, or replacing existing systems; increased public confidence in modified or replacement systems) against the attendant costs (e.g.; immediate cost of replacing existing systems; maintenance problems, security risks, and public doubts associated with existing systems). The

FEC recommends that either automatic or manual audit trail and security capabilities, as described in the technical standards, be incorporated with all voting systems in use by January 1992. States may want to consider financial aid to local jurisdictions as an incentive to modify or replace existing systems.

3.2.4 Encouraging the Use of High Level Language

There was disagreement among technical experts as to whether or not the standards should require the use of high level language in voting system software. Furthermore, election officials expressed concern that they would be required to replace perfectly good software written in assembly language with high level language programs, if the

standards required high level language. This, in turn, might necessitate the concomitant purchase of new hardware. Voting system vendors also were concerned about establishing such a requirement. They maintained that they would be forced to rewrite all existing programs and that the use of high level language would significantly reduce the speed of the vote tabulation, thereby raising the suspicions of election observers. Technical experts did agree, however, that programs written in a high level language are easier to test due to their well-known, uniform methods of issuing computer commands.

In attempting to balance conflicting opinions, the FEC decided that the use of high level language in voting system software is desirable, but not required. Instead, the FEC urges the states to adopt measures to promote the use of high level language in key portions of voting system software that is developed in the future. It is hoped that the use of high level language will draw more independent test authorities into the process of evaluating computerized voting systems.

The FEC recommends that states set a date (e.g.; January 1996) after which new voting system software first submitted for qualification must use high level language for those portions of system software associated with the logical and numerical operations on vote data. States should continue to permit the use of assembly language for input/output routines, however. States should also permit local jurisdictions to continue using assembly language software that was shown to comply with the standards before 1996 and that conforms to state requirements.

Exhibit A _ Recommended Implementation Timetable

January 1990 The FEC's voluntary voting system standards are formally released.

Vendors continue efforts to develop new voting systems or modify existing systems to comply with the standards.

States begin efforts to adopt all or portions of the FEC standards.

Local jurisdictions procuring new voting systems begin to investigate vendors' plans to upgrade or replace any systems currently marketed that do not comply with the proposed state standards.

January-June 1990 Several states begin adopting all or portions of the FEC standards. Provisions for acceptance testing and escrow are effective immediately in these states. Vendors begin submitting new or modified systems to test authorities for qualification.

January 1991 A number of states have adopted all or portions of the FEC standards.

January 1992 States that adopted new standards by early 1990 begin certifying only systems that comply with the technical standards.

Local jurisdictions procuring new systems within these states select only from this pool of certified systems.

All voting systems in use incorporate, automatically or manually, minimum security and audit trail capabilities described in the technical standards.

No later than this date, vendors cease marketing systems not designed to comply with the new state standards.

Exhibit A _ (Continued)

January 1996	After this date, all computerized voting systems in use within the states comply with the new state standards. Also after this date, all voting system software first submitted for qualification testing uses high level language in the portions associated with logical and numerical operations on vote data.

3.3 The Enabling Vehicle

States may choose to implement the standards in one of three possible ways: by administrative fiat, by regulation, or by statute. Each avenue has advantages and disadvantages.

Administrative fiat allows the chief election official of the state the greatest flexibility _ making it possible to quickly implement and easily revise the standards without legislative intervention. Since a public notice or comment period is not normally required, the effective date is not delayed. One problem associated with this approach is that not all state election officials are empowered to use this method. Certainly, if questions arise concerning the statutory authority to implement standards via administrative rule, legal challenges to voting system procurement decisions are possible.

The regulatory route, while granting the state election official some control over implementation and an ability to revise the standards with relative ease, is often impeded by public notice and comment periods as well as possible legislative objection.

The statutory process, though the least adaptive, may in some states may be the only politically acceptable alternative. The normally slow legislative process, however, inhibits both the swift enactment and the speedy revision of standards. It may even invite partisan squabbles over essentially technical issues. The process also allows election officials the least control over how the standards will be implemented. Still, should the statutory process be the only available route, it maybe possible to design legislation which would merely empower the chief election official to establish such standards for voting systems and procedures for implementing them as may from time to time be necessary.

3.4 Alternative Approaches to Adopting the Standards

Some states intend to adopt the minimum federal standards in their entirety. Others plan to review the standards item by item and implement only those relating to a specific type of voting system (punchcard, marksense, or direct recording electronic) or only those which seem most pertinent to the needs of the state. Some states may choose to adopt the standards by reference. Others may integrate the wording for each standard into the election code, applicable regulations, or administrative rules.

States should be aware of existing state law governing their actions, if any. They should also consider the merits and drawbacks associated with each approach, and the decisions required.

3.4.1 Adopting the Standards Substantially Intact

States intending to adopt the standards with little or no change should concentrate on both the standards for voting system performance and the requirement for acceptance tests. The escrow plan and relevant portions of this implementation plan should also be reviewed and their proposals incorporated accordingly.

States will need to determine an effective date for the performance standards, a date after which any systems presented for certification or acquisition should comply with the standards. In recognition of the time needed for product development, the FEC recommends that states set an effective date approximately two years after the adoption date. The requirement for localities to conduct acceptance tests on newly acquired systems, however, may be implemented immediately. Escrow provisions adopted by the state may also become effective immediately and may be extended to existing systems in use.

States do not need to explicitly adopt the qualification test and measurement methods because these specifications will automatically be used by independent test authorities when conducting national qualification tests on new systems. It is appropriate, however, that states require that all systems certified or acquired after the specific effective date of the standards be examined by a test authority for conformity to these standards. States may also specify that the results of these tests should be considered during review of any new system for state certification.

3.4.2 Adopting the Standards Selectively

States choosing to adopt the standards selectively also need not concentrate on the qualification test and measurement methods, though they should indicate state recognition of the results of a national examination. Instead, these states should focus on the performance standards, the acceptance test guidelines, this implementation plan, and the escrow plan.

States which elect to adopt only those standards related to specific voting system types (punchcard, marksense, or direct recording electronic) will most likely do so to cover the types of systems legally permitted in their state at the time. States choosing this approach should recognize that their standards must be revised if another type of voting system is subsequently permitted. These states might do well to adopt standards for other systems if legislative approval of these systems is imminent.

States which intend to employ an item by item approach to the FEC performance standards should consider the ramifications of rejecting any minimum standards or requiring any optional ones. States electing either approach would be wise to document the reasons for their decisions.

States that choose to delete any standard should note carefully all places in the FEC standards document where that standard is referenced. For example, states that do

not want to implement the requirement for independent processing paths in DRE systems must recognize that the decision affects the functional, hardware, software, and security sections of the standards. Whether the remaining standards are adopted by reference or incorporated in toto, the sections or language of the FEC document that should be deleted must be marked.

3.4.3 Adopting the Standards by Reference

States may adopt the standards by reference, if state administrative procedure laws and related case law permits. This approach will likely save substantial printing costs. If this is done, however, a decision should be made as to whether or not FEC amendments to the standards will be adopted automatically.

If subsequent amendments are to be incorporated without prior state review, the reference may state, for example:

No computerized voting system may be certified or acquired (or used) after (date) that does not meet the standards adopted by the Federal Election Commission on (date), specifically Sections through (or pages through), as they may be amended time to time; and that has not been tested by an independent test authority to confirm compliance.

The merit to this approach is that amendments will be integrated without delay. The obvious drawback is that the state waives its right to determine if the amended standards are appropriate. In some states, this approach would constitute an illegal delegation of state legislative authority to an agency outside of the state. Therefore, before considering this approach, the state should determine whether or not the state constitution and statutes permit it.

The alternative approach would require states to review amendments as they are issued and decide whether or not to adopt them. The initial enabling language might be similar to that cited above, with the phrase regarding amendments deleted. Instead, another sentence could be added stating: Future amendments will be considered for adoption by (responsible state officer or state body) on a case by case basis.

The advantage to this approach is that it ensures that a state agent will review the amended standards to verify that they are appropriate for that state. The disadvantage is that the process is more cumbersome and, depending on the enabling vehicle, may be very time consuming.

3.4.4 Integrating the Full Text of the Standards

Some states may be required by state law to incur the cost of printing the full text of any standards adopted. It is likely that this cost will be substantial. States taking this

approach should plan their budget in order to account for the cost of printing both the initial standards and any subsequent amendments adopted.

3.5 Adopting Other Recommendations

In addition to the FEC standards, states should consider reviewing and adopting recommendations from other relevant sources. The National Institute of Standards and Technology, for example, has issued a report entitled Accuracy, Integrity, and Security in Computerized Vote-Tallying that proposes additional administrative safeguards and voting system requirements. Also, a non-profit organization named ECRI has issued a two volume report entitled An Election Administrator's Guide to Computerized Voting Systems. This report, released subsequent to the testing of several voting systems by ECRI, contains recommendations for system procurement.

3.6 The Impact of the Preclearance Provisions of the Voting Rights Act on Implementation

The Voting Section in the Civil Rights Division of the Department of Justice has informed the FEC that, with regard to the implementation of the standards, there will be a pro forma process for states which fall under the preclearance provisions of the Voting Rights Act. Although these states must still submit legal or procedural changes affecting elections to the Department of Justice, the review process will likely be expedited.

4.0 The Application of Standards to Various Categoriesof Voting Systems

The FEC does not recommend that the FEC performance, design, and test standards be applied equally to all categories of voting systems. The FEC also does not recommend that states follow the same certification procedures for all categories of systems. From a practical standpoint, different categories of voting systems require different treatment according to the time and origin of their development and the extent to which they have been used and tested.

There are, broadly speaking, two major categories of voting systems discussed below: Vendor-developed systems, and In-house developed systems.

Within each of these major categories are equally important subcategories including: existing systems, which we define as those not originally developed to be in compliance with the standards, many of which are currently in use; modified existing systems, which we define as being existing systems modified to be in partial or full compliance with the standards subsequent to initial state certification. new systems, which we define as those developed to be in compliance with the standards and which are first marketed or, if developed in-house, used after the FEC standards were issued (i.e., 1990 or later); and modified new systems, which we define as being new systems modified subsequent to qualification testing;

The following subsections propose an approach for applying the standards to each of these categories and subcategories.

4.1 Vendor-Developed Systems

Vendor-developed systems fall into the four main subcategories:

Existing Systems.

Modified Existing Systems.

New Systems.

Modified New Systems.

The following sections suggest how the standards might best be applied to each subcategory.

4.1.1 Existing Vendor-Developed Systems

The FEC does not recommend that performance and design standards be applied to existing systems in use. As suggested above, vendors should be encouraged to modify

these systems to comply with the standards or, at least, to incorporate minimum security measures and audit trails. If it is not feasible to modify an existing system, local jurisdictions should be encouraged to employ administrative procedures to provide system security and audit trails.

National Qualification Testing for Existing Vendor Developed Systems

The FEC does not suggest that full qualification testing, as described in the standards, be conducted on existing systems. It is recommended, however, that some voting systems presently in use be submitted for examination. The rigor of the examination should be commensurate with the extent to which the hardware or software has been previously tested and used.

Systems previously examined by an independent organization (e.g.; ECRI, SRI, a big eight auditing firm) and which have not exhibited significant problems may not require testing unless they are subsequently modified. Such systems, in effect, have been evaluated to some extent and have been proven in the field. (See Section 4.1.2 for a discussion of qualification testing of modified existing vendor developed systems.) Systems not previously examined should be examined by a state auditor, outside technical consultant, or independent test authority. This review should include ballot logic and system-level functional tests so that any areas of undiscovered marginal performance can be identified. Vendors may, of their own volition, choose to submit these systems for examination or each state or, alternatively, a group of states may submit such systems to examination before state certification.

State Certification Testing for Existing Vendor-Developed Systems

Particular attention should be given to how the state will certify existing systems. Certification test criteria for these systems will likely be more rigorous than for new systems because they will not have demonstrated compliance with all minimum performance standards.

States that have established a certification authority that has worked well in the past may use the same process to address existing systems. Those states that have not established a reliable procedure are strongly encouraged to establish a bipartisan certification board whose membership includes persons with data processing and legal expertise. This board should review any test reports available, establish certification test criteria, oversee the conduct of any necessary certification tests, evaluate test results and, if necessary, hire an outside consultant who is not connected with a vendor to design or conduct the tests.

States should consider certifying and permitting the purchase of existing systems up until time the standards become effective for system procurement, even if these systems do not yet comply with the standards. Local jurisdictions that are in need of another system before the effective date will have little from which to choose if existing systems are prohibited. Furthermore, vendors may not have the capital needed to modify existing systems or develop new ones if states bar them from

marketing their systems during this time. States and local jurisdictions would then have fewer systems that do meet the standards from which to choose in the future.

States reviewing existing systems for certification may request that vendors provide information on what prospective modifications, if any, are planned to bring the system into partial or full compliance. States will, most likely, examine the system again once the modifications are made. (See State Certification Testing for Modified Existing

Vendor Developed Systems in Section 4.1.2 below.)

Local Acceptance Testing for Existing Vendor-Developed Systems

The FEC recommends acceptance testing for all newly acquired voting systems. These tests are usually performed by the local jurisdiction, sometimes with the assistance of an outside consultant. Yet, states may be well advised to determine their role, if any, in the acceptance testing of existing systems. In particular, states should decide whether or not they will provide written guidance to, oversee, or directly assist local jurisdictions in their conduct of acceptance tests.

Direct state assistance may take the form of technical or financial aid. Oversight may involve the observation of acceptance testing by a technical representative of the state. Written guidance may include the recommendation that local jurisdictions gather the expertise necessary to conduct and evaluate acceptance tests (i.e.; a contract officer or lawyer to evaluate compliance with the contract, technical data processing personnel to set up a test plan, hardware and software specialists, and enough technicians to conduct the tests) and a reference to the types of tests which should be conducted.

If the state is not involved with conducting acceptance tests, the local jurisdiction should design an appropriate test plan and conduct tests, in consultation with technical experts such as county/city data processing personnel, vendors, approved independent test authorities, and private consultants.

4.1.2 Modified Existing Vendor-Developed Systems

Existing systems may be modified, either to correct defects, to bring the system into partial or full compliance with the standards, or to enhance the system. Modified existing systems (e.g.; those retrofitted to provide audit trails) should be required to meet only those minimum standards that relate to that modification.

National Qualification Testing for Modified Existing Vendor-Developed Systems

The vendor should submit any existing system that has undergone either software or hardware modifications to an independent test authority (ITA) for examination. The FEC, however, does not recommend that full system qualification testing as required by the standards be performed on these systems. Furthermore, none of the hardware

tests need be performed on modified existing systems unless the ITA determines that hardware modifications are of such consequence as to affect functionality.

The ITA will decide what testing is required based on the type of modification, how the modification affects the system's function, the past performance of the original system in field use, and what documentation exists of previous tests performed on the original system and the modified system. The vendor should provide pertinent documentation to the ITA to assist in this process including but not limited to: vendor test data, test data from independent organizations and states, the vendor's certification of compliance with specific standards, and documentation of the specific modifications.

ITA assessment of the modification should be completed at least 45 days prior to the modified system's use in an election. The resulting ITA report should contain an assessment of the modifications and define what action, if any, has been taken. The report should be sent to the vendor with a copy going to the FEC Clearinghouse. It should be the vendor's responsibility to send copies of the ITA report to the states notified of the modification and to local jurisdictions that may utilize the modification.

State Certification Testing for Modified Existing Vendor-Developed Systems

States should examine modified existing systems to ensure their compliance with state code. States may decide to review documentation on modifications, conduct functional ballot logic tests, and, if hardware has been modified, review human engineering factors.

The decision to retest should be influenced by the ITA report, the extent of the modification, and whether or not the system has previously been certified for use in the state. Modified existing systems may well require closer scrutiny than modified new systems. Nevertheless, states are urged not to duplicate tests already conducted by the ITA or another state.

States should consider who will decide to what extent modified existing systems should be examined and whether or not the system complies with state requirements.

In doing so, states should have access to legal and technical personnel to assist with the review of the ITA report.

States may also wish to consider how they will deal with vendors who market modified systems in their jurisdiction which have not been reviewed by the ITA or the state. Options states may choose include decertifying the system, levying monetary penalties, or initiating criminal sanctions against the vendor.

Local Acceptance Testing for Modified Existing Vendor-Developed Systems

Acceptance testing required for modified systems will vary according to the extent of the modification and whether or not the local jurisdiction is acquiring the modification for their previously procured and tested system or is acquiring the modified system as

a whole to replace or augment the voting system currently used. Extensive and system-wide acceptance testing should be performed on whole systems initially procured after modification.

For systems modified subsequent to procurement, local jurisdictions may need to conduct either partial or full acceptance tests depending on the nature of the change. The decision to conduct new tests or repeat previous tests should include consideration of whether hardware was retrofitted or software upgraded. The tests may concentrate on the areas affected by the modification.

The states should determine whether or not they will provide direct assistance, oversight, or written guidance for acceptance testing of modified existing systems.

4.1.3 New Vendor-Developed Systems

There is no foreseeable end to the growing technical sophistication of voting systems. Indeed, it is precisely because of this trend that the FEC standards have been devised. The primary objective of the standards is to ensure that voting systems designed and marketed in the future will meet the standards necessary to maintain confidence in them. Because the most populous states are expected to adopt at least the minimum standards, it is anticipated that new systems developed by vendors in the foreseeable future will meet all of the minimum standards described in the Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems.

If a vendor contemplates or is developing a new system that does not follow the general practice for voting systems addressed by the FEC standards, the vendor should prepare design requirements and specifications for the new system that conform to the functional requirements and performance levels established by the standards. These specifications should be submitted to the FEC for review. During product development, the vendor should also submit the Technical Data Package, described in Appendix B of the standards, to the FEC. The Commission will negotiate confidentiality agreements to protect the proprietary interests of the system developer. The Commission will then update the standards to cover the new system and issue the revised standards to states. This process will help ensure system acceptability, without adding undue delay in the introduction of new system types or configurations to the market place.

National Qualification Testing for New Vendor-Developed Systems

The FEC anticipates that new systems developed by a vendor will be submitted to all required qualification tests specified in the standards. In addition, the optional, and more expensive, qualification tests (e.g.; rain exposure or sand and dust exposure) will

likely be performed unless the states inform the FEC that they are not required before systems are submitted for state certification.

These tests will be conducted by an independent test authority (ITA) and the resulting report will provide the ITA's opinion of the system. The ITA report should identify the specific environment in which the testing was done, describe the test plan, and present the results of tests performed and the ITA's evaluation of system software design.

If a jurisdiction requires that systems under consideration be tested against more rigorous standards, the additional tests of each system should be performed by the same ITA that conducted the original qualification tests of that system. These tests should be arranged through all potential vendors and a copy of the resulting test reports should be filed with the FEC. The test reports will then be available for review by other interested jurisdictions.

State Certification Testing for New Vendor-Developed Systems

States should consider defining certification tests for new, qualified systems in a manner which would avoid duplicating the qualification tests. States can contact the

FEC for copies of current qualification test reports. The FEC urges states to confine certification tests to those needed to demonstrate the system's ability to meet specific state requirements (e.g.; those governing ballot format, ergonomics, and vote counting). The states may also allow the certification process to recognize relevant tests already performed by other participating states in order that those tests might not be repeated.

States should identify what documentation will be required for this examination and who will be responsible for conducting the certification review. At a minimum, the vendor's system documentation and the test results and conclusions contained in the ITA report, including the test authority's opinions on the quality of the hardware and software design, should be considered.

Local Acceptance Testing for New Vendor-Developed Systems

Local acceptance testing prior to contractual acceptance of new systems is highly recommended. The object of this testing is to determine if the hardware or software delivered complies with state and local requirements and performs in accordance with the same equipment's performance in qualification testing. Local jurisdictions should have access to technical expertise, either at the state or local level, when designing a test plan, performing the tests, and analyzing the results.

States should consider their role in acceptance testing of new systems, especially whether or not they will provide written guidance, oversee, or directly assist local jurisdictions in conducting acceptance tests on these systems.

4.1.4 Modified New Vendor-Developed Systems

It is likely that new systems may eventually be modified, after submitting to qualification testing. Modifications may be made to enhance the system, or even to correct a defect. The FEC anticipates that all modifications to new systems will comply with the minimum standards.

National Qualification Testing for Modified New Vendor-Developed Systems

Any change to a new system should be examined by an independent test authority.

The vendor, ideally, should use the same ITA that conducted the qualification testing of the original system. The test authority will review documentation and vendor test data to assess the modification's impact on system functions, and to determine the extent of retesting required.

Depending upon the circumstances, the ITA may subject new systems with software modifications to:

Software qualification tests, including functional ballot logic tests and audits of code and documentation; and

System-level qualification tests, including physical and functional configuration audits and functional system performance tests.

New systems with hardware modifications may be subjected to:

Hardware qualification tests, including a qualitative examination and environmental operating and non-operating tests; and

System-level qualification tests, including physical and functional configuration audits and functional system performance tests.

Under certain circumstances, if the change does not affect demonstrated compliance with the standards, a performance test may be all that is necessary.

ITA assessment of the modification should be completed at least 45 days prior to the system's use in an election. The resulting ITA report should contain an assessment of the modifications and describe what action, if any, was taken.

State Certification Testing for Modified New Vendor-Developed Systems

States should examine modified new systems to ensure that they comply with state requirements. If the state previously certified the original system, subsequent recertification may not require additional tests on site. Instead, a review of the ITA report and the vendor's documentation of the modification may be sufficient. Any decision to test a modified new system should take into account tests already performed by the ITA.

States should designate who will decide to what extent modified new systems should be examined and what documentation is needed. States should also establish the

timetable to be followed from the release of the ITA report through the announcement of the state's certification decision and the incorporation of the modification by local jurisdictions.

States may also wish to consider what sanctions to apply to vendors who might market modified new systems that have not been reviewed by the ITA or the state.

Options states may choose include decertifying the system, levying monetary penalties, or initiating criminal sanctions against the vendor.

Local Acceptance Testing for Modified New Vendor-Developed Systems

Local jurisdictions will need to conduct either partial or full acceptance tests of modified new systems, depending on the nature of the change and whether or not the local jurisdiction is only enhancing their system with the modification or acquiring the modified new system as a whole. When determining what testing is required, local jurisdictions should take into account tests previously performed on the system.

Full acceptance testing should be performed if the jurisdiction is acquiring the modified system as a whole. On the other hand, tests may be concentrated on the areas affected by the modification if the system was previously subject to acceptance testing and the modification is limited. The local jurisdiction should have access to technical expertise either at the state or local level to assist in this process.

States should determine their role, if any, in this decision process and the conduct of needed tests (i.e.; whether or not they will provide written guidance, oversight, or direct assistance in acceptance testing of modified new systems).

4.2 Systems Developed In-House

Systems developed in-house fall into the same four subcategories as vendor developed systems:

Existing systems.

Modified existing systems.

New systems.

Modified new systems.

4.2.1 Existing Systems Developed In-House

Existing systems developed in-house are not expected to comply with the performance and design standards. As stated earlier, local jurisdictions should be encouraged to eventually replace or modify these systems to bring them into full compliance or, at least, to incorporate critical security measures and audit trails. If system modification is not feasible, local jurisdictions should be encouraged to implement administrative procedures to secure the system and provide the audit trails described in the standards.

Testing and State Oversight for Existing Systems Developed In-House

The FEC does not recommend that national qualification testing be conducted on existing systems developed in-house. State certification similar to that of vendor-developed systems is also not anticipated. The FEC does, however, recommend that these systems be examined by a state auditor or outside technical consultant and that ballot logic and system-level functional tests be performed to identify any areas of undiscovered marginal performance.

States will also want to identify what systems developed in-house are in use in their jurisdiction, and monitor their examination and modification or replacement. Suggested procedures for monitoring modifications follow.

4.2.2 Existing Systems Modified In-House

Existing systems developed in-house may be modified, either to correct defects, to enhance the system (e.g.; to add modules to interface with ballot tally programs), or to bring it into partial (e.g.; to provide audit trails) or full compliance with the standards. Modified existing systems, including those under continuous development, generally should be expected to meet only those minimum standards which apply to the modification.

Testing and State Oversight for Existing Systems Modified In-House

Existing systems modified in-house should be tested during and after the modification process, but, should not be expected to submit to full qualification testing. Instead, these systems should be examined by a state auditor or outside consultant hired by the state or local jurisdiction. The examiner will determine if further testing is necessary.

States will want to monitor the modification of existing systems for compliance with state standards. States may require local jurisdictions to report anticipated or completed modifications. States may also employ one or more of the following methods of monitoring modifications:

Recording reported changes.

Reviewing system test data from tests performed in-house or by an outside contractor.

Reviewing the completed modified product.

Reviewing throughout the entire modification process.

Providing technical assistance to the jurisdiction during software modification.

4.2.3 New Systems Developed In-House

The performance and design standards are intended to apply fully to systems developed in-house and first used after the effective date of the standards as set by the state.

Testing and State Oversight for New Systems Developed In-House

The FEC anticipates that new systems developed in-house will be subject to qualification testing under the standards. The FEC recommends that, at a minimum, these systems be subjected to the functional and physical configuration audits, source code review, and ballot logic and system-level functional performance tests described

in the standards. The tests should be conducted either by state auditors or outside consultants hired by the state or local jurisdictions. The examiner would, most likely, review the software and local test documentation and conduct appropriate qualification tests on-site.

State oversight during development may be appropriate in lieu of the formal system certification process. States will want to consider establishing a reporting system to enable the detection and examination of new systems under development in-house.

The FEC recommends that local jurisdictions be required to report any new systems under development in-house to the state. In addition, states may wish to employ one or more of the following methods to monitor the development of these systems for compliance with state adopted standards:

Recording reported developments.

Reviewing system test data from tests performed in-house or by an outside contractor.

Reviewing the completed product.

Reviewing throughout the entire development process.

Providing technical assistance to the jurisdiction during the software development process.

The system should be subject to acceptance testing by the local jurisdiction, after qualification testing but prior to its use in any election.

4.2.4 New Systems Modified In-House

New systems developed in-house may be modified subsequent to qualification or acceptance testing. Modifications may be made to enhance the system, account for a change in state ballot counting procedures, or even to correct a defect. The performance and design standards are intended to fully apply to modified, new systems including those under continuous development.

Testing and State Oversight for New Systems Modified In-House

New systems modified in-house should be tested during and after the modification process to ensure that the system continues to comply with the standards and state and local requirements. The modified system should be examined and tested either by state auditors or outside consultants hired by the state or local jurisdictions.

States will want to monitor the modifications of new systems for compliance with state standards. States may require local jurisdictions to report anticipated or completed modifications. States may also employ one or more of the following methods to monitor modifications:

Recording reported changes.

Reviewing system test data from tests performed in-house or by an outside contractor.

Reviewing the completed product.

Reviewing throughout the entire modification process.

Providing technical assistance to the jurisdiction during the software modification.

5.0 Evaluating Test Authorities

The role of the independent test authority in the implementation of the voting systems standards is a crucial one. Test authorities will make the initial determination of how well voting systems comply with the standards, and thus will ultimately judge the system's accuracy, security, and dependability. Therefore, a test authority's expertise and impartiality are important factors. It is important, then, that vendors select competent independent test authorities (ITAs) able to conduct qualification tests of their voting system hardware and software.

It is also important that state and local election officials consider the chosen test authority as credible so that they will not demand repeated qualification testing. This objective can best be achieved if a national authority provides an unbiased evaluation of test authorities as an aid to vendors when making their selection.

Because a central, federally assisted evaluation process is not possible without both Congressional appropriation of necessary funds and time to develop evaluation criteria, some method must be used to identify potential independent test authorities in the interim. In order not to delay issuance and state implementation of the voting systems standards, the accompanying paper A Process For Evaluating Independent

Test Authorities is being released with short and long term recommendations for this effort. If a formal federal evaluation process is not established, vendors will still need criteria to assist them in selecting ITAs that are both competent and acceptable to states.

The proposed evaluation process will assist vendors in identifying test authorities best able to apply the FEC voting system standards. It will also promote greater uniformity and stability among test authorities and reduce the possibility of repeated qualification testing of voting systems. States will be more certain that tests of voting systems have been executed according to a baseline set of national standards. States may, therefore, be less likely to require vendors to submit their voting systems to duplicate and expensive tests during state certification.

Throughout this process the FEC will attempt to enlarge the pool of available test authorities willing and able to conduct qualification tests. To date, only a limited number of organizations have expressed an interest in conducting qualification testing due to the complexities involved.

5.1 The Need for a National Program

States cou1d adopt their own individual ITA evaluation programs. This option, however, seems very costly and repetitive. Fifty separate assessment procedures would result in a needless duplication of effort. Numerous bodies of this nature, whether informal or otherwise, would also be tremendously cumbersome. Nor is coordination even among small groups of states very likely owing to the oftentimes

varied and unique political circumstances within each state. It is also likely that all states would not as readily accept test results from test laboratories evaluated in this manner.

The FEC explored private and public sector alternatives and sought the opinions of vendors and state election officials. Respondents overwhelmingly recommended that the process be coordinated by an independent and unbiased third party and, for reasons of credibility, rejected private associations in favor of a federal agency that would be responsible for the evaluation process.

The FEC subsequently approached the National Voluntary Laboratory Accreditation

Program of the National Institute of Standards and Technology (NVLAP/NIST), which is the federal agency experienced in laboratory accreditation and statutorily authorized to perform such formal assessments. NVLAP/NIST has agreed to assist the FEC in estab1ishing broad assessment criteria that may be employed by voting system vendors in their selection of test authorities. (This segment of the program is hereafter referred to as Phase I.)

Should further funds become available through Congressional appropriations or private foundation grants, NVLAP/NIST will build on this initial criteria to establish a formal ITA accreditation program (Phase II). It is envisioned that a NVLAP accreditation program would assess the test authority's internal quality control procedures, test facilities and equipment, key personnel, and knowledge of and experience with appropriate test procedures by means of a formal application process. Applicants would be required to certify that no conflict of interest exists between them and any voting system vendor. Technical experts would evaluate potential test authorities in accordance with the technical criteria through: information supplied by the ITAs in their application, the results of the proficiency tests, and on-site visits. Vendors could then select a test authority from among those that have received NVLAP accreditation.

Neither the vendor-applied ITA evaluation criteria nor the more formal NVLAP accreditation program can guarantee that work performed by the chosen test authorities will be error free. They can, however, provide some assurance that the selected ITAs are regarded as capable of adequately testing voting systems and that there is no conflict of interest.

5.2 Interim Selection of Test Authorities

Until and unless a formal NVLAP accreditation process is established, the FEC recommends that vendors submit their voting systems to one of the major accounting/consulting firms or universities generally recognized across the country as competent in evaluating computer systems. This vendor selection process might be undertaken in consultation with various states.

Local firms are not recommended in the interim because of their lack of widespread recognition and credibility among various states. This might increase the likelihood that states would reject the test plans and results. Such rejection would either exclude that vendor from subsequent competition in those states or compel a costly re-testing for voting system qualification by a recognized test authority.

Qualification testing of a single voting system may be performed by one test authority, but may also may be conducted by different testing bodies that specialize in various aspects of hardware and software evaluation. Whenever more than one organization is involved in qualifying a voting system, the FEC recommends that voting system vendors designate a single test authority as coordinator. This prime contractor should create the test plan, subcontract appropriate tests, collect the test results, and prepare the final report consolidating the test results and presenting the overall system assessment. The prime contractor should assume full responsibility for the independence and competence of all subcontractors.

The FEC, if Phase I is completed, will recommend criteria that vendors may use to evaluate nationally recognized, potential test authorities. These criteria may be issued by August 1990. If an accreditation program is established in Phase II, vendors may select from any accredited test authority. The FEC Clearinghouse will maintain a

list of test authorities interested in conducting qualification tests. If Phase II is completed, a list of those accredited by NVLAP will also be available through the FEC Clearinghouse.

5.3 Phase I _ Initial Development of Evaluation Criteria

During the proposed Phase I, the FEC will develop an overall plan and, with NVLAP/NIST assistance, identify technical experts representing both government and private sector interests. The technical experts will develop baseline technical evaluation criteria in consultation with NVLAP/NIST and the FEC. While this developmental process is underway, the FEC will contact potential ITAs in an effort to expand the field of those interested in conducting voting system qualification testing.

Prospective ITAs and voting system vendors will likely be involved in the formulation

of the technical criteria. The proposed guidelines will be discussed in public meetings and formally issued to voting system vendors for their use. The FEC will also provide copies of the guidelines to states for informational purposes.

5.4 Phase II _ NVLAP Accreditation

During the proposed Phase II, NVLAP will build upon the work accomplished in Phase

I, assisted by the technical experts. The broader spectrum technical criteria developed in Phase I will be analyzed by NVLAP specialists and refined to provide more elaborate or in-depth qualitative assessment measures.

The scope of the technical accreditation criteria will be dependent on both time and available funds. Accordingly, NVLAP proposes an incremental approach whereby detailed technical criteria can be established first in key areas such as software code analysis for logical correctness and accuracy. After development of these "narrow" criteria, actual accreditation limited to this critical area could proceed. Depending on the availability of funds, additional criteria could be similarly established and integrated with successive accreditation and periodic ITA review processes.

NVLAP personnel and technical experts will develop related ITA proficiency testing programs at the same time as the assessment criteria is being developed. These sample tests provide a formal mechanism for NVLAP off-site assessment of an ITA's hands-on testing capabilities.

Although funding is needed to develop the detailed protocols that would be used in

NVLAP accreditation, the program should be virtually self-sufficient once the criteria and proficiency tests are established if there are enough applicants for accreditation. Applicants for accreditation would pay a fee which would cover the costs of administering the program.

6.0 The Escrow Process

The FEC recommends that states adopt procedures for escrowing software system documentation for all voting systems _ existing, new, and modified vendor-developed systems, as well as voting systems developed in-house. The proposed process requires the vendor to deposit specified materials with an escrow agent, an independent party who acts as a neutral third party between the vendor and user. As modifications or improvements are made to the baseline system configuration, the vendor notifies the escrow agent who is responsible for monitoring this periodic update process.

Under defined situations, the escrow agents forward source code and other needed materials, in a secure manner, to the designated test authority for qualification testing. Should state election offices need certain materials for state certification, these would be forwarded to the appropriate authority in like manner. Upon completion of testing, all materials would be sealed and sent back to the escrow agent who then documents receipt of the originally released materials.

6.1 Benefits to Escrow

The escrow process, as proposed, contains many potential benefits for both vendors and users. An escrow agent, in his normal course of operations, has the physical and security safeguards for sensitive and proprietary materials. Legal guidelines provide clear-cut scenarios for access to sensitive materials that protect the interests of both vendors and users; the escrow agent is prohibited from unilaterally releasing materials. The monitoring and updating of master deposits as systems are modified is assured by the escrow agent.

State and local jurisdictions would have guaranteed access to all deposit materials as a last resort in the event a vendor's business fails. Ultimate accountability and responsibility would increase as well. Vendors or users could compare software used in the vote count to the archived version of the software deposited in escrow to determine if authorized modifications had been made.

If the escrowed materials had been adequately reviewed and tested by an independent test authority (ITA) and directly sent to the escrow agent, it is likely that the archived software would be error free. The escrow process then allows for verification of software used in an election against the clean archival copy. In the event of litigation, a court of competent jurisdiction could ask for and receive the escrowed executable code for ultimate verification in a controlled setting against the installed version actually used to conduct the election. It must be clearly understood, however, that the escrow of system documentation and software does not prevent an election from being compomised, nor does it ensure error free code.

6.2 Choice of Escrow Agent

The FEC has identified several escrow companies that provide a wide range of services. The possibility always exists that more vendors may enter the market. States may wish to enter into escrow agreements before the standards go into effect. In most instances, the vendor will select an escrow company, since they will pay initial deposit costs and maintenance fees. In other instances, the user might select an escrow company, based on the guidelines set forth in the System Escrow Plan for the Voting System Standards Program, and then instruct the vendor to deposit specified materials with that company.

6.3 Types of Escrow Agreements

The FEC recommends the adoption of "multiple-user" agreements, rather than separate and distinct contracts. The former reduces the number of agreements involved, and ultimately the costs, among vendor, escrow agent, state, and local jurisdictions.

From a security standpoint, it is necessary to restrict access to potentially sensitive computer files and documentation to a limited number of persons. For this reason, the FEC recommends that the state level election authority function as registrant in the escrow process on behalf of the local jurisdictions. The registrant is the ultimate recipient of released escrow materials. Because state authorities are generally not responsible for the programming of election software, their possession of this information minimizes any potential appearance of impropriety.

The FEC recommends that states not make the source code or other potentially sensitive materials concerning security available to jurisdictions unless it is absolutely necessary.

6.4 Deposit Contents

The FEC recommends that the escrow agreement include an essential provision that obligates the vendor to deposit into escrow all materials needed to enable a knowledgeable third party to maintain the system under conditions of bankruptcy or abandonment. Specifically, the deposit should contain all necessary computer files and documentation such that an exact copy of a run-time program model can be produced from the source code, should it be needed.

A comprehensive list of items that should be deposited into escrow is contained in the System Escrow Plan for the Voting Standards Program. States, however, should note that vendors may not have all the documentation relating to older systems (with the exception of source code). Therefore, the list of items requested by states to be deposited into escrow might have to be adjusted accordingly for these systems.

6.5 Triggering Events and Release Conditions

States should examine the proposed triggering events (i.e.; occasions which allow the user to initiate procedures to gain access to the deposit) and select the ones most appropriate for their own particular set of circumstances. States should understand that the occurrence of a triggering event does not automatically translate into release of the deposit to the user. Where possible, negotiations should be conducted with the vendor before any material is formally requested from escrow. Under this scenario, the state or local jurisdiction will notify the escrow agent that it feels entitled to the release of the deposit. In turn, the escrow agent will send a "release request" to the vendor. Should the vendor decide not to challenge the request, the deposit (or portions thereof) would then be released.

Nothing contained in the escrow process is intended to preclude the immediate release of pertinent deposit materials to a criminal investigative tribunal (e.g., a grand jury) or upon order of court in a criminal proceeding.

6.6 State Law Applicable to the Escrow Process

By itself, an order from a court of competent jurisdiction may be sufficient to compel the escrow company to release the source code to the user. As an added measure designed to ensure access across state boundaries particularly during litigation, the FEC recommends that the state designate the Secretary of State (or another official in charge of corporations) as the in-state representative of the escrow company in legal matters. The FEC also recommends that the escrow company be licensed to do business within all states in which there are subscribers.

6.7 Protection of Escrowed Material During Legal Action

The refusal of either vendor or user to accept some form of binding arbitration in disputes over access to the deposit could make court action unavoidable. States should, therefore, take all reasonable steps to ensure the confidentiality of escrowed material released to the courts. Specifically, states may want to consider the use of in-camera proceedings when election related proprietary information is involved. At a more general level, states should consider giving cases involving access to source code and other proprietary documentation the same high priority assigned to other election matters.

6.8 Open Record Laws

Most states do not exempt trade secrets. Although Freedom of Information laws may not apply when states and local jurisdictions are not directly involved and the material

is held by a neutral third party, it is critical that states examine specific provisions of their laws from the standpoint of restricting access to this proprietary information.

All states, and particularly those with jurisdictions that choose to keep proprietary information on site, should consider a means of excluding the ballot counting source code and other propriety documentation from the state's Freedom of Information act or open records laws.

Several states have tried to limit the scope of public domain through a variety of means. Texas law, for example, requires that source code and other proprietary documentation which is filed with the Secretary of State be exempt from public scrutiny. In some instances, case law or Attorney General opinions may achieve the goal of keeping the information confidential. Arizona, for example, enacted an exemption based on an Attorney General's opinion using the "best interest of the state" test. Op. Att. Gen. No. R75-721. p. 47, 1976-77.

6.9 Time-Frames for Escrow Deposit

For security and control purposes, the vendor shall place all required items into deposit prior to submitting any system to qualification testing.

The same time-frame requirement holds for updates to escrow deposits that reflect modifications to systems. Test authorities would receive all or a portion of the information needed to test the system from the escrow agent. The escrow agent would be responsible for sealing and shipping this information under controlled conditions. Any computerized files would be properly labeled for identification.

Since outdated source code or documentation is generally recognized as having little value to the user, the FEC recommends that the vendor notify the escrow agent in the event of any update. It is strongly recommended that updates be submitted at regular intervals, at least yearly or preferably more frequently. The exact number of updates will depend, of course, on the maturity of the system. If the vendor has made no changes to the system at the end of a twelvemonth period, the escrow company should be duly notified. Generally, escrow updates must be made well in advance of the election (at least 60 days) in order to allow the test authority sufficient time to examine the material and report its findings.

7.0 Information Flow

This section describes the flow of information among the seven participants involved in implementing the standards. While the paper flow necessary for the success of this standards program may at first glance seem complex and onerous, its purpose is actually to simplify and facilitate communications. To this end, the FEC proposes to use its Clearinghouse for the exchange and dissemination of pertinent information regarding status of all voting systems nationwide.

7.1 The ITA Evaluation Process

During the developmental stage of Phase I, the FEC will contact potential ITAs in an effort to expand the field of those interested in conducting voting system qualification testing. The FEC will maintain a list of these test authorities and make it available to all interested persons.

After broad technical ITA evaluation criteria are identified in Phase I, the FEC will issue them to voting system vendors for their use in selecting a test authority. The

FEC will also provide copies of the guidelines to states for informational purposes.

If a NVLAP accreditation program is later initiated (Phase II), NVLAP/NIST will provide and accept applications for accreditation. NVLAP/NIST will notify the applicant directly if a deficiency must be corrected before accreditation can be granted. NVLAP/NIST will provide accredited test authorities with an accreditation certificate and will notify the FEC when a test authority is accredited or loses accreditation. A list of those accredited by NVLAP will be available through the FEC Clearinghouse.

7.2 The Escrow Process

Vendors should deposit the specified software items and documentation with an escrow agent. The proprietary information will be made available to users only if needed.

States and local jurisdictions should decide and document what events may trigger the release of the executable code, source code, or other information. If the user believes that a release condition has been met and seeks to review the deposit, it will so inform the escrow company. The escrow company, in turn, will send a “release report” to the vendor. Any user who obtains previously escrowed material is obligated to maintain its confidentiality and to return it to the escrow company once the particular problem has been resolved.

The state should serve as the agent of the escrow company for the purposes of receiving summons or subpoenas during contested elections. The state should, of course, notify the escrow company promptly of any such action. If a third party serves any of the entities with a complaint, subpoena, or motion for discovery involving the escrowed deposits, all parties should be notified within five days of the action (unless more immediate action is warranted under the circumstances).

If escrowed material is obtained through legal action, the material must be protected from public scrutiny and returned to escrow when no longer needed.

7.3 The National Qualification Test Process

For new systems, vendors should handle proprietary information and its submission to the escrow company in the following manner:

The vendor will place in escrow all specified materials prior to submitting a new or modified new voting system to an ITA for qualification. The escrow agent will be responsible for forwarding the needed information to the designated ITA in a secure, controlled manner. Once testing is completed, the escrow materials will be sent directly back to the escrow company. The escrow agent will track and document all items and the deposit in this transfer process.

The original of the ITA report will be forwarded directly to the escrow company, where it will be an update to the deposit, separately available upon request. Copies of the ITA report will be transmitted to the vendor and the FEC.

The vendor will provide the report to the jurisdictions where they plan to market the system. The FEC will disseminate this information to other interested states or jurisdictions when the information is requested by them.

7.4 The State Certification Test Process

In states where the vendor seeks certification, the vendor should distribute the ITA qualification test report. Based on this report and the specific requirements of state law, the state should design and conduct certification tests. States are encouraged to provide the FEC with copies of certification test plans and reports. The FEC will make this information available to other states and interested persons. The states should also make the qualification and certification test results available to local jurisdictions within the state that are interested in acquiring the system.

7.5 The Local Acceptance Test Process

Local jurisdictions should obtain copies of qualification and certification test reports from the state. The local jurisdiction, with or without assistance from the state, should plan and conduct acceptance tests on procured systems. Local jurisdictions are encouraged to provide the FEC with copies of acceptance test plans and reports.

This information will be made available to other jurisdictions or interested persons.

7.6 Systems in Use

States are encouraged to inform the FEC regularly of what systems (vendor and in-house developed) are in use, newly purchased, or under development in-house. Local jurisdictions are encouraged to report similar information to the state. This provision will enable states to track systems in use and monitor the in-house development of new systems. The FEC will make this information available to interested persons including jurisdictions seeking to purchase new voting systems or upgrade existing ones.

7.7 Modified Systems

Vendors should notify the states that have certified their system of any modifications to that system. Local jurisdictions that have acquired the system should be similarly notified. The escrow agent and the FEC Clearinghouse should also be informed of the modification. The notices to states, local jurisdictions, the FEC, and the escrow agent should contain information such as: a summary of what changes the vendor made, to which ITA the vendor sent notification of the modification, the estimated time frame for the ITA examination, and the date after which the results of the ITA review are likely to be available.

The ITA will review the modification and forward the resulting report to the vendor and the FEC Clearinghouse. The vendor will be responsible for providing the test report to the appropriate states and local jurisdictions.

If the ITA obtains material from the escrow company for the purpose of testing modifications, such materials shall be returned directly to the escrow company after test completion. If the vendor provides additional information for the test, the ITA will also return the vendor-supplied information to the escrow company.

If system modifications span an extended period of time, the vendor should decide when and how often to notify the ITA, the states, the Clearinghouse, and the escrow agent of the status of the modifications. For a mature system, the vendor should contact the ITAs and escrow agent at least yearly to state whether or not the system has been modified.

If the modification requires state recertification, and it is approved, states are encouraged to inform the FEC. Local jurisdictions that acquire the modification are encouraged to inform the state which, in turn, should notify the FEC of that fact.

States may require local jurisdictions to report anticipated or completed modifications to systems developed in-house. State may request local jurisdictions to provide related documentation and test data to facilitate state review of the modification. The FEC urges states to notify the Clearinghouse of in-house modifications when they are implemented.

-

SYSTEM ESCROW PLAN

FOR THE

VOTING SYSTEM STANDARDS PROGRAM

FEDERAL ELECTION COMMISSION

JANUARY 1990

APRIL 1990 REVISIONS TO THE SYSTEM ESCROW PLAN

Section 1.0

This section has been rewritten to clarify the objectives of employing an escrow process.

Section 5.0

In Subsection 5.2, the second paragraph has been revised to state that security documentation must be deposited in the event the vendor chooses not to deposit

all documentation required by the technical standards. Also, the security penetration analysis has been specifically listed under the Software Specification items that must be deposited in escrow under this option.

Section 7.0

The third sentence in Subsection 7.1 was deleted as it was considered an unnecessary statement.

Subsection 7.6 has been revised to clarify that legal action to release the escrow deposit may encompass both civil and criminal litigation.

TABLE OF CONTENTS

Page

Page

SYSTEM ESCROW PLAN

1.0 Background

During the development of the standards, a number of questions arose concerning access to sensitive information, such as voting system software and documentation. The Federal Election Commission (FEC) began looking for a method to secure this information without denying access needed by independent test authorities and users. Technical consultants to the FEC suggested a formal escrow process, which is widely used in commercial industry. In this sphere, the escrow process is routinely used to monitor software versions, to enable system maintenance when the vendor fails to provide adequate support, and to protect the vendor against liability charges for third party mistakes.

In-depth discussions on the applicability of the practice to elections revealed other important advantages. First, it became clear that once a test authority had completed qualification testing of a voting system, the related software and documentation could be forwarded directly to an independent escrow agent. Any software subsequently installed could then be verified against the clean archival copy in the event of contested elections or criminal investigations of alleged fraud. Second, the process provides a formal means of monitoring the various updates to system software. Vendors would be required to periodically notify the escrow agent of modifications,

and to send appropriate materials for deposit. Third, the escrow system would centrally safeguard materials that might be needed by a number of users if the vendor fails to support the system. Fourth, the practice would contribute to the security of voting systems by controlling access to sensitive items that could be used to compromise them.

2.0 The Escrow Process

In short, escrowing involves the vendor deposit of source code, object or executable code, documentation and other materials with an escrow agent, an independent party who acts as a neutral third party between the vendor and user. As modifications or improvements are made to the baseline system configuration, the vendor notifies the escrow agent who is responsible for monitoring this periodic update process.

Under defined situations, the escrow agents forward source code and other needed materials, in a secure manner, to the designated test authority for qualification testing. Any materials state election offices need for state certification will be forwarded in a like manner. Upon completion of testing, all materials shall be sealed and sent back to the escrow agent who then documents receipt of the originally released materials.

If the escrow materials have been adequately reviewed and tested by an independent test authority (ITA) and directly sent to the escrow agent, it is likely that the archived software is error free. The escrow process then allows for verification of software used in an election against the clean archival copy. In the event of litigation, a court of competent jurisdiction could ask for and receive the escrowed executable code for ultimate verification in a controlled setting against the installed version actually used to conduct the election. It must be clearly understood, however, that the escrow of system documentation and software does not prevent an election from being compromised, nor does it ensure error free code.

3.0 Protection for Both Users and Vendors

The FEC recommends that users of both vendor and in-house developed systems familiarize themselves with the many potential advantages of escrow. The escrow process provides additional protection that makes it more beneficial than the simple deposit of materials in a vault. Primarily, the escrowing of software, equipment specifications and documentation addresses two key concerns:

- The verification of correct software installation with previously tested and archived executable files; and
- The provision of necessary computer files and information to permit the user continued use and maintenance of the system in the event of manufacturer bankruptcy or failure to service the system.

Several surveys undertaken by the FEC in 1987 and 1988 found many state and local jurisdictions believing that their interests could best be served by actual possession of vote tallying source code. In reality, absent explicit statutory exclusions, escrowing may be more desirable than actual possession. The user's physical possession of the source code and other proprietary documentation may allow public access to that information under Freedom of Information statutes. This same access by local authorities could call into question the the security and integrity of the electoral process.

An escrow agent, in his normal course of operations, has the physical and security safeguards for sensitive and proprietary materials. Legal guidelines provide clear-cut scenarios for access to sensitive materials that protect the interests of both vendors and users; the escrow agent is prohibited from unilaterally releasing materials. The monitoring and updating of master deposits as systems are modified is assured by the escrow agent. Under an escrow plan, state and local jurisdictions shall have guaranteed access to all deposit materials as a last resort in the event a vendor's business fails. In contrast, deposit of materials with an attorney or a bank is not likely to provide the full range of services available through commercial escrow processes.

4.0 Types of Escrow Agreements

The FEC recommends the adoption of "multiple-user" agreements, rather than separate and distinct contracts. The former reduces the number of agreements involved, and ultimately the costs, between vendor, escrow agent, state, and local jurisdictions. It is simply inefficient for each state and local user to rely upon separate contracts when comparable systems and software versions may be installed in numerous localities.

Two principal types, or levels, of agreements are employed under the multiple-user concept. The first type involves agreement between individual vendors and the selected escrow company or companies. Depending on the number of distinct voting systems, the vendor negotiates separate master agreements with the escrow company and agrees to make one deposit per system. Within this master agreement, different versions and releases can be indicated, thus eliminating the need for many separate contracts. All materials to be placed in this master deposit are described later in this document. Appendix B outlines a sample agreement between vendor and escrow company.

For those systems currently in use, the vendor will provide to the escrow agent a list of those local jurisdictions within each state using the specific system configuration. The escrow agent then proceeds to register the respective state jurisdictions to the appropriate master agreement.

The second level of multiple-user agreement takes place between states and the escrow company (or companies). The FEC recommends that each state authority serve a primary role in the escrow process as registrant. In this capacity, the state shall prescribe conditions relative to the contents of escrow deposits, frequency of updates, replacements to deposit, and on behalf of the local jurisdictions would dictate the specific triggering clauses and release conditions. Appendix E of this document contains several sample documents relating to provisions for verification, replacement of deposits, and release conditions.

Thus, a separate written contract is required where the state is registrant to the agreement and the local users are signed on to the agreements as subscriber jurisdictions. Appendix C contains a sample agreement to this effect.

There are several benefits to this arrangement in addition to cost savings:

- Smaller jurisdictions that do not have local expertise can have the state to act on their behalf;
- The state may wish to reserve access to materials before subscriber jurisdictions have negotiated purchase contracts; and
- States that take an oversight role in the contracting and maintenance process may wish to have triggering conditions of their own.

Should a specified condition arise where the deposit (or portions of it) is to be released, its contents shall be forwarded to the state authority (as registrant) and not to the numerous local jurisdictions. Thus, limitations on the number of recipients and security over potentially uncontrolled access to sensitive material is minimized.

5.0 Contents of Deposit

The FEC recommends that the escrow agreement include an essential provision that obligates the vendor to deposit into escrow all material needed to enable a knowledgeable, third party to maintain the system under conditions of bankruptcy or abandonment.

Specifically, the deposit shall contain all necessary computer files and documentation such that an exact copy of a run-time program module can be produced from the source code, if it is needed.

Several terms relating to deposits warrant definition:

- Source code _ consists of text files containing program statements which, when compiled and linked, result in an executable software program; composed of two generic categories: vote tally software and, optionally, data entry software for precinct count systems that produces election specific firmware.

- Object code _ consists of binary machine instructions produced by a compiler (or assembler) operating on source code; these machine instructions are unique to the particular microprocessor being used.
- Executable file _ composed of object code (file) linked together with necessary support functions contained in library or utility files.
- Library files _ collections of support functions for a specific compiler or source code. Without these files (also called utility files), one cannot properly link object code to produce the executable program.

5.1 Required Software Items

The following is a generic list of software files that the vendor must place in deposit for each system and software release. Indicated is the form in which this data shall be submitted:

- all vote tallying source code, in written form, shrink-wrapped in volumes;
- all vote tallying source code, in electronic form, encrypted;
- all data entry-ballot preparation source code, in written form, shrink-wrapped in volumes;
- all data entry-ballot preparation source code, in electronic form, ASCII format, encrypted;
- compiler listing of source code including cross reference listing of functions, global and local variables, system calls, library routines, memory maps, and label tables;
- separate enclosure containing de-encryption key(s) for all application source code;

- all executable files for vote tallying software, in electronic form, nonencrypted;
- all executable files for ballot preparation software, in electronic form, non-encrypted;
- written identification (name, version number) of the commercial compiler;
- written identification (name, version number) of the commercial operating system;3
- specially designed compilers, in electronic form; and
- library files, in electronic form.

These various deposits items, in both electronic and paper form, will provide multiple sets of data to meet the anticipated needs of parties in litigation, in contested elections, or other general disputes. The simultaneous deposit, under separate cover, of the de-encryption key provides for an extra level of security and enables the compilation of source code into executable or run-time code for verification purposes. The printed listing of program source code enables test authority review of the design and logical correctness of the source code.

With these various computer files deposited in escrow, it is the explicit intent of the FEC that executable code (not source code) be used for verification and for litigation purposes, and importantly, that strict controls over the indiscriminate release and access to source code be in force and strictly monitored.

5.2 Required System Documentation

Appendix B of the standards contains the Technical Data Package (TDP), an exhaustive inventory of documentation that the vendor must provide prior to system qualification. In general, the TDP contains system developmental test data, design approaches, system hardware specifications, system software specifications, and user operating and maintenance manuals.

Two different approaches for the deposit of the TDP into escrow can be taken. Unless the state authority dictates otherwise, it is the vendor's responsibility to select one of the following two options. Vendors may either place into escrow all documentation required by the standards, or only the security documentation and those manuals and segments of other documentation directly applicable to state and local system testing and maintenance. In either instance, such items as the Approved Parts List, technician service manuals, and schematic system diagrams shall be included in the deposit.

This second option excludes system developmental data and qualification test specifications required by the test authority but not normally needed by the user jurisdiction. With this second option, the following items shall be submitted to the escrow agent as part of the master deposit:

- Hardware Specification:

System Definition

System Characteristics System Support Requirements

- Software Specification:

System Overview
Program Description
Operating Environment
Software Functional Specification
_ Overview
_ Configuration and Operating Modes _ External Files
_ Operational Security
Security Penetration Analysis

- Acceptance Test Specification
- System Operating Manual
- System Maintenance Manual

In addition to the formal documentation requirements, the vendor should also deposit, if applicable, the following information:

- Descriptions and locations of other associated programs not owned by the voting system vendor;
- Names and addresses of the system programmers; and
- A list of users of the particular system(s).

6.0 Conditions Triggering Escrow Release

The escrow agreement shall specify all events that may trigger release of the escrowed material—those catastrophic occurences that may initiate release to the state as registrant. This section is, perhaps, the most important part of the escrow agreement between the state and escrow company. Because of the likelihood of disputes between vendor and user, the rights and obligations of each must be outlined as clearly as possible. It must be emphasized that the call for release of deposit materials will be initiated only as a last resort.

From the user's perspective, initial system installation, subsequent upgrades, training, and continuing support are issues of highest priority. Hence, the escrow agreement shall include specific support conditions to be provided by the vendor and precise definitions of catastrophic events involving "failure to support." The specific support provisions should also be included in the purchase/lease agreement.

Failure to support provisions are included in the escrow agreement to allow the state

(or local) user access to the pertinent material so that the system or software can be maintained without the support of the third party vendor. While the exact wording of these provisions will be ultimately determined by the state in consultation with their local jurisdictions, it is possible that the provisions might:

- require that the vendor repair or replace within a stated time frame any failed or deficient software and hardware;
- provide technical assistance and on-sight personnel during system acceptance, installation, pre-election day testing, election night operations and recount; and
- provide for training of state and local personnel in the proper operation and maintenance of the system.

The escrow agreement may also include some of the following examples or definitions of failure to support:

- Bankruptcy or termination of the vendor's business;
- Physical disaster to the vendor's maintenance facilities that adversely affects the company's ability to support the system; and
- The departure of one or more the key software developers or testers that adversely affects prescribed maintenance schedules.

Additionally, the escrow agreement shall include clauses designed to protect the user in the event that either party breaks the agreement. It is conceivable that the vendor, for instance, might merge with another company and then decide no longer to maintain the system. Special attention must be paid to clearly outlining rights and responsibilities in this type of situation due to the intangible, i.e., intellectual, nature of software. If properly handled, potential problems can be minimized.

The parties may wish to include in the escrow agreement an additional triggering condition commonly used in the commercial software environment: allowing the user to gain access to the escrowed material if the vendor attempts to sell, pledge, assign or transfer such material in a manner which conflicts with the rights granted under the agreement. It is left up to the states' discretion whether or not to make this provision mandatory. By including this clause, the user would be protected in the event that the vendor pledged the source code as collateral for a loan. Should the vendor

subsequently find himself in default, the lender (i.e., bank) may take possession of the escrowed material.

7.0 Escrow and Purchase Agreement Clauses

The FEC recommends that the terms of the escrow agreement be incorporated into the purchase/lease agreement since this may be the only legal document defining vendor obligations that is signed jointly by the vendor and the purchaser. The purchase/ lease agreement also should include a clause specifying the specific contents of the deposit to be placed in escrow.

Due to the sensitive nature of the material and the conflicting priorities of users and vendors, the escrow agreement will require delicate negotiations between the parties. In particular, special attention must be given to the following areas:

- Applicable State Law • Fee Arrangements
- Release Time
- Release Conditions
- Arbitration
- Legal Action

7.1 Applicable State Laws

The purchase/lease agreement, as well as the escrow agreement, shall specify which state laws apply and under what circumstances. For example, if laws of the user state apply in gaining access to the escrowed material, this should be stated. As an added measure to ensure access during litigation, the FEC recommends that the escrow company be licensed to do business in all fifty states, and that the state designate the Secretary of State (or another official overseeing corporations) as the agent of the escrow company solely for purposes of litigation.

Finally, in addition to requiring the escrow company to be bonded, the user also should be compelled to post bond
with the court in the event the court releases the deposit and later reverses itself and finds that the user is, in fact, not
entitled to the information.

7.2 Fee Arrangements

With regard to fee arrangements, the FEC recommends that vendors and users consider sharing escrow fees so as
to avoid placing an undue financial burden on either party. Accordingly, it is suggested that the vendor pay for all

the initial deposit costs plus the initial maintenance fees. Those state jurisdictions wishing to escrow shall be indicated as registrants to the master vendor deposit. Local jurisdictions may sign on as subscribing jurisdictions to these agreements. Local jurisdictions will pay annual subscription fees.

Should the state or local jurisdiction need additional services, such as system verification, then the user could absorb the costs. Obviously, the exact fee for services rendered will depend upon the technical complexities presented. Also, in order to ensure the continuous deposit of the escrowed material, the user must be allowed to pay escrow fees where the vendor has failed to do so. Finally, while the actual schedule of payments ultimately will be determined by the parties involved, state and local jurisdictions may consider allocating escrow costs over an extended period, perhaps three to five years, in order to reduce actual costs.

7.3 Release Time

The escrow agreement must provide some means to ensure that the escrow agent cannot choose to hold the deposited material for an unjustifiable length of time while the vendor and user (state or local jurisdiction) attempt to resolve any differences over the possible release of source code. As a possible solution, the escrow agreement may allow the user access by injunction. The requesting party shall be required to post a bond and be responsible for damages if the source code is disclosed, or not eventually returned.

7.4 Release Conditions

States will rarely need to trigger release of source code in order to conduct certification tests since an exhaustive examination would have already been performed by the ITA.

The occurrence of a triggering event, furthermore, will not automatically release the deposit to the user. In most cases, if the state or locality feels entitled to actual possession, it will inform the escrow company. In turn, the escrow company will send a "release report" to the vendor. If the vendor refuses access, arbitration may result.

The FEC recommends that the escrow agreement clearly outline the responsibilities of the state authority under conditions of release. Once the problem has been solved, the state shall be required to return the deposit to the escrow company.

The escrow company shall notify other state registrants whenever there is actual release of any materials in deposit.

7.5 Arbitration

It is possible that the vendor will object to the user's gaining access to sensitive materials in deposit. Relying on the courts to resolve these differences can be expensive and time consuming. Thus, such conflicts should be handled through an abbreviated arbitration proceeding. The escrow and purchase agreements should call for arbitration. During this process, each side presents its case to an arbitration board shortly after the dispute has arisen. The board, usually consisting of three members appointed by the two disputants, decides quickly since the issue of access is the only one at hand.

In order to save a party from defending a lawsuit in a remote court, the arbitration clause also may specify a mutually convenient location for the arbitration board. The addition of a mutual liquidated damages provision may simplify matters even further and cause software owners and users to exercise extreme caution in situations involving the release of source code.

7.6 Legal Action

While the FEC recommends that escrow disputes be resolved through arbitration, the refusal of parties to accept binding arbitration may make civil action unavoidable. In addition, an order by a criminal investigative tribunal (e.g., grand jury) will result in immediate release. In these events, the possibility of partial, or even complete public disclosure of source code and sensitive materials, like the security penetration analysis, increases dramatically. Accordingly, additional steps must be taken to ensure the confidentiality of the material. The escrow company will only release a copy of the original deposit materials. In all instances, the recipient of the copy shall take all precautions to secure and protect them. When the court proceedings are completed, the recipient shall destroy the materials received from escrow, rather than return them.

The vendor shall authorize the escrow company and the user jurisdictions to take any necessary legal steps to prevent sensitive material from being indiscriminately released. Whenever sensitive or proprietary election information is involved in any court case, the FEC strongly recommends using in-camera proceedings (where allowed under state law). A new requirement which Texas has included in a statute, reads as follows:

The materials may be made available in a judicial proceeding on the request of the court or other tribunal but may be viewed in-camera only.

The parties shall incorporate a notification clause into the escrow agreement requiring that if a third party serves any of the contracting parties with legal process, all the other parties (including the FEC) will be notified within five days of service (unless more immediate action is warranted under the circumstances). Such a procedure will aid in the protection of the proprietary documents by keeping all interested parties properly informed.

Moreover, states must consider giving cases involving access to the source code and other sensitive documentation the same high priority assigned to other election matters.

8.0 Timing of Escrow Deposits

For security and control purposes, the vendor shall place all required items into deposit prior to submitting any system to qualification testing. This condition holds only if the vendor has placed into deposit all the information called for in the standards. The vendor may have to forward any additional information to the test authority in the event that only selected items had been deposited into escrow.

The same time-frame requirement holds for updates to escrow deposits that reflect modifications to systems. Test authorities will receive all or a portion of the information needed to test the system from the escrow agent. The escrow agent shall be responsible for sealing and shipping this information under controlled conditions. Any computerized files must be properly labeled for identification.

Since outdated source code or documentation is generally recognized as having little value to the user, the FEC recommends that the vendor notify the escrow agent in the event of any update. It is strongly recommended that updates be submitted at regular intervals, at least yearly or preferably more frequently. The exact number of updates will depend, of course, on the maturity of the system. If the vendor has made no changes to the system at the end of a twelve month period, the escrow company shall be duly notified. Generally, escrow updates must be made well in advance of the election (at least 60 days) in order to allow the test authority sufficient time to examine the material and report its findings.

The vendor may, at his discretion, choose to have a system reviewed on a periodic basis. In this case, the same paper flow from the escrow agent to the test authority shall hold.

9.0 Trade Secrets and Open Records Laws

Vendors and users, alike, are concerned with the need for adequate security, protection of trade secrets, and maintaining the integrity of the voting system.

States are urged to address this issue in light of their Freedom of Information statutes or other "open records" laws. Under such laws, the possibility exists that business competitors may gain access to the source code or other proprietary documentation filed with the state. Several states are attempting to limit the scope of "public domain." Texas, for example, recently passed legislation requiring that source code and other documentation be filed with the Secretary of State and that such material be exempted from public scrutiny. The relevant sections of the measure read as follows:

Sec. 122.0331. ADDITIONAL REQUIREMENT FOR ELECTRONIC VOTING SYSTEM.

Copies of the program codes and the user and operator manuals and copies or units of all other software and any other information, specifications, or documentation required by the Secretary of State relating to an approved electronic voting system and its equipment must be filed with the Secretary.

> The program codes and all other software on file with the Secretary of State under this section are not public information.

Other states have enacted restrictions as part of original public records legislation. Illinois, for example, has the following provision as one of its exemptions:

Sec. 7.9. Trade secrets and commercial or financial information obtained from a person or business where such trade secrets or information are proprietary, privileged or confidential, or where disclosure of such trade secrets or information may cause competitive harm. Nothing contained in this subsection shall be construed to prevent a person or business from consenting to disclosure.

Most states, unfortunately, do not expressly exempt trade secrets. Yet all states, including those which do not adopt an escrow arrangement, must consider a means for excluding sensitive election computer files and documentation from the state's open records laws. At the least, judges should be made aware that the release of source code and security provisions involves the potential for security and fraud violations. In some instances, case law or Attorney General Opinions may achieve this goal of confidentiality. Arizona, for example, exacted an exception based on an Attorney General's Opinion using the "best interest of the state" test.

Op. Atty. Gen. No. R75-721, p. 47, 1976-77.

As an added step aimed at restricting access to those who have a need to know, the vendor may want to request that user jurisdiction employees (state and local) sign confidentiality, non-disclosure agreements.

10.0 The Escrow Company

In consultation with the states, the vendor shall select an escrow agent and deposit all specified materials. It is hoped that vendors will negotiate with states if a

change in escrow companies is desired. Currently, four escrow companies have been

identified:

- Data Securities International, Inc. _ California
- National Safe Depository _ California
- Software Escrow Security _ Massachusetts
- The Vault Company _ Georgia

Rather than recommend any one escrow company, the FEC has developed guidelines that may be used in making a selection:

1. The company selected shall be an independent neutral third party having no direct or indirect financial interest with the vendor.
2. The company shall be staffed with technical experts capable of system installation, deposit verification, and administration of the contract agreement with multiple subscribers and registrants.
3. The company shall be bonded and licensed to operate in all fifty states.
4. The company shall promise not to disclose the source code and documentation unless it is specifically allowed to do so under the terms of the escrow agreement.
5. The company shall provide a multiple-user system with master agreements between the vendor and the escrow company and a second series of agreements between the escrow company and the user(s).
6. The company shall perform, as needed, the following functions (using in-house staff so as not to jeopardize confidentiality):
    a. Visual inspection of the contents of the deposit including tally source code, operating systems, and run-time application files, to determine compliance with the contract provisions.
    b. Comprehensive audits and reference checks of all software and system maintenance documentation.
    c. Installation of the software on independent system hardware and performance of software comparison tests to verify locally installed software object code against the source code in the escrow deposit.
7. The company shall provide humidity and temperature control on a 24hours-a-day, 7-days-a-week basis.

Appendix A

Sample Clauses for Software Preservation

Appendix A

Sample Clauses for Software Preservation

Article

Non-disclosure: [Escrow Company] agrees that, except as provided in this Agreement, it, its officers, directors, or employees, will not disclose, divulge or otherwise make available to any third party, or in any way use for its own purposes, any information provided to it by Vendor in connection with this Agreement, without the express written consent of Vendor.

Article

Absence of any pecuniary interest in Vendor: [Escrow Company] hereby

warrants that it [its officers] [and directors] [individually and severally] hold or exercise no pecuniary interest(s) in Vendor, and that Vendor [its officers] [and directors] hold

or exercise no pecuniary interest(s) in [Escrow Company]. [Escrow Company] agrees to advise all [Jurisdictions] of the information provided to it by Vendor in connection with this Agreement within ten days of the effective date of the perfection of such pecuniary interest.

Article

Indemnification: [Jurisdiction] agrees to defend and indemnify, and otherwise

hold [Escrow Company] harmless against all claims, of whatever nature, incurred by [Escrow Company] on account of any act or omission of [Escrow Company] in connection with this Agreement, except for those detailed in Article(s) [ ], [ ], and [ ].

Article

Indemnity Bond: [Escrow Company] agrees that it will secure and maintain [an] indemnity bond(s) with respect to each [Jurisdiction] of the information delivered to

it by Vendor under this Agreement, and will be liable under such bond(s) for acts or omissions detailed under Article , above.

Appendix B

Sample Agreement Between Vendor and Escrow Company

Appendix B

Sample Agreement Between Vendor and Escrow Company

Account Number

This Software Deposit Agreement ("Agreement") is effective this day of , 198 , by and between (Escrow Company) a (State) corporation and (Vendor)

WHEREAS, Vendor has or will enter into a contract(s) with persons or corporation(s) ("Jurisdiction(s)") for the use of computer software and other materials:

WHEREAS, availability of or access to proprietary data related to the computer software and other materials is critical to certain Jurisdictions in the conduct of their business:

WHEREAS, Vendor has deposited or will deposit with (Escrow Company) the related proprietary data to provide for retention and controlled access for certain Jurisdictions under certain conditions:

NOW THEREFORE, for good and valuable consideration, the receipt of which is hereby acknowledged, and in consideration of the promises, mutual covenants and conditions contained herein, the parties hereto agree as follows:

Article 1

Definition of Deposit. The initial Deposit of proprietary data consists of any and all material supplied by Vendor to (Escrow Company) pursuant to this Agreement (including amendments hereto), as specified in the "Description of Deposit Materials."

The Deposit will include any supplemental materials which may be added to the Deposit from time to time by Vendor pursuant to this Agreement. Such supplemental materials to the Deposit will be added by an Amendment to this Agreement accompanied by a "Description of Deposit Materials."

Definition of Registered. Vendor agrees to submit and execute a "Registration to Deposit Account" (Exhibit A) for each jurisdiction to be covered under this Agreement. Such Jurisdiction shall hereafter be referred to as a Registered Jurisdiction.

Addendum for Subscribed Jurisdictions. Vendor, and only Vendor, may addend this Agreement in order to define the rights of a Subscribed Jurisdiction by executing a "Jurisdiction Subscription Document." (Exhibit B) (Escrow Company) shall permit Subscribed Jurisdictions to this Agreement only upon acceptance of the Jurisdiction Subscription Document.

Subscribed Jurisdiction. Vendor, and only Vendor, may enroll certain Jurisdiction(s) as Subscribed Jurisdiction(s) after an accepted Jurisdiction Subscription Document. Vendor must execute and submit to (Escrow Company) an "Enrollment of Subscribed Jurisdiction(s)" listing each Jurisdiction to be Subscribed under this Agreement. Upon acceptance of an "Enrollment of Subscribed Jurisdiction(s)" by Escrow Company and payment of the subscription fee(s), Jurisdiction(s) will be a Subscribed Jurisdiction(s).

Article 2

Replacement of Deposit. Vendor may from time to time replace the Deposit with replacement materials. Vendor shall submit such replacement materials (as modifications, new versions, or new editions) to (Escrow Company) by Amendment to this Agreement and a new "Description of Deposit Materials" describing such materials. Such replacement materials shall be treated by (Escrow Company) as required in the case of the initial Deposit.

(Escrow Company) will, absent any contrary provision in any "Registration to Deposit" (Exhibit A) to this Agreement, at Vendor's option either destroy or return to Vendor such replaced Deposit.

(Escrow Company) shall be under no obligation to accept any replacement materials for deposit unless accompanied or preceded by a duly executed Amendment to this Agreement and a "Description of Deposit Materials" (Exhibit B) describing the replacement materials pertaining thereto.

Article 3

Obligations of (Escrow Company). (Escrow Company) agrees to accept the Deposit referred to in Article 1 in accordance with this Deposit Agreement. (Escrow Company) agrees to establish a receptacle in which it will place the Deposit, and will put the receptacle under the control of one or more of its officers, selected by (Escrow Company) from time to time, whose identity shall be available to Vendor at all times. (Escrow Company) will exercise that high level of care in carrying out the terms of this Agreement as (Escrow Company) would use to protect items of this nature which (Escrow Company) might own.

(Escrow Company) shall bear no obligation or responsibility whatsoever to determine the existence, completeness, or accuracy of the Deposit. (Escrow Company) shall have no obligation or responsibility to determine whether what is

deposited is or is not proprietary data as defined or contemplated herein.

Article 4

Term of Agreement. This Agreement shall have an initial term of year(s). This Agreement may be renewed for additional year periods upon receipt by (Escrow Company) of the specific renewal fee. In the event that the renewal fee is not received on or before the expiration date, (Escrow Company) shall so notify Vendor, all Registered Jurisdictions and the Federal Election Commission. A Registered Jurisdiction or Jurisdictions shall have the right to pay the renewal fee in the event of Vendor's default.

Under no circumstances shall the Federal Election Commission be responsible for any of the fees generated by the Vendor, Jurisdictions of (Escrow Company) . Further, the Federal Election Commission is not a party to this agreement and shall not incur any liability for the actions of the parties involved in this agreement. If the fee is not received within the subsequent thirty (30) days, this Agreement shall expire without further notice and without liability to any other party.

Article 5

Expiry. Upon expiry or non-renewal of this Agreement, all duties and obligations of (Escrow Company) to Vendor hereunder shall terminate. (Escrow Company) will, at Vendor's option, either destroy or return to Vendor the Deposit unless otherwise provided for in this Agreement.

In the event that a Registered Jurisdiction pays the renewal fee pursuant to notice received under Article 4 (Escrow Company) will notify Vendor and if Vendor is of the opinion that any necessary condition for renewal is not met, Vendor may so notify Commission in writing within thirty (30) days of receipt of payment by (Escrow Company) . The resulting dispute shall be resolve pursuant to the Dispute Resolution Process defined in the "Registration To Deposit" (Exhibit A) for that Registered Jurisdiction.

Article 6

Delivery of Deposit. In the event that (Escrow Company) is notified by a Registered Jurisdiction of the occurrence of a release condition as defined in the "Registration to Deposit" (Exhibit A) for that Registered Jurisdiction, (Escrow Company) shall so notify Vendor and the Federal Election Commission and shall provide a copy of the notice from Registered Jurisdiction. If Vendor provides contrary instructions, as defined in this Article within ten (10) days of the mailing or other service of the notice to Vendor.

copy of the Deposit to the Registered Jurisdiction demanding delivery. If no contrary instructions are received, (Escrow Company) will deliver a copy of the Deposit to Registered Jurisdiction demanding delivery.

Contrary instructions for the purposes of this article means the filing of an affidavit or declaration with (Escrow Company) by Vendor, with a copy to

Registered Jurisdiction demanding delivery, and stating that a Release Condition has not occurred, or had been cured. Upon receipt of contrary instructions, (Escrow Company) shall not deliver a copy of the Deposit and will continue to store the Deposit until otherwise directed by Jurisdiction and Vendor jointly, or until resolution of dispute pursuant to the Dispute Resolution Process defined in the "Registration to Deposit" (Exhibit A) or by a court of competent jurisdiction.

Article 7

Release Conditions. Release conditions shall have the meaning(s) ascribed thereto in the "Registration To Deposit" (Exhibit A).

Article 8

If any of the Documentation held in escrow by (Escrow Company) shall be attached, garnished or levied upon pursuant to a court order, or the delivery thereof shall be stayed or enjoined by a court order, or any other order, judgment or decree shall be made or entered by any court affecting the Deposit or any part thereof or any act of (Escrow Company) in its sole discretion to obey and comply with all orders, judgments or decrees so entered or issued by any court, without the necessity of inquiring whether such court had jurisdiction, and in case order, judgment or decree (Escrow Company) shall not be liable to any Registered Jurisdiction, Vendor or any third party by reason of such compliance, notwithstanding that such order, judgment or decree may subsequently be reversed, modified or vacated.

Article 9

Non-Disclosure. Except as provided in this Agreement, (Escrow Company) agrees that it will not divulge or disclose or otherwise make available to third parties or make any use whatsoever of the Deposit, or any information provided to it by Vendor or Registered Jurisdiction in connection with this Agreement or exhibits, without the express prior written consent to Vendor or Registered Jurisdiction, as the case may be. Notwithstanding the above provision, (Escrow Company) shall release the names of Vendor and Registered Jurisdiction(s) to this Agreement to the Federal Election Commission within thirty (30) days of the signing of this Agreement.

Article 10

Indemnification. Vendor agrees to defend and indemnify (Escrow Company) and hold (Escrow Company) harmless from and against any and all claims, actions, and suits, and from and against any and all liabilities, losses, damages, costs, charges, penalties, counsel fees, and other expenses of any nature (including, without limitation, settlement costs) incurred by (Escrow Company) on account of any act or omission of (Escrow Company) in respect to or with regard to this Agreement except as specified in Articles 4 and 10.

Article 11

Audit Rights. (Escrow Company) agrees to keep complete written records of the activities undertaken and materials prepared pursuant to this Agreement.

Vendor shall be entitled at reasonable times during normal business hours and upon reasonable notice to (Escrow Company) during the term of this Agreement to inspect the records of (Escrow Company) with respect to this Agreement.

Vendor shall be entitled, upon reasonable notice to (Escrow Company) and during normal business hours, to inspect at the facilities of(Escrow Company) the physical and technical status and condition of the Deposit.

Article 12

Designated Representative. Vendor agrees to designate an authorized individual to receive notices and otherwise act on behalf of Vendor with respect to the performance of its obligations under this Agreement.

Article 13

General. (Escrow Company) may act in reliance upon any instruction, instrument, or signature believed to be genuine and may assume that any person purporting to give any writing, notice, request, advice or instruction in connection with or relating to this Agreement has been duly authorized to do so.

This Agreement shall be governed by, and construed in accordance with the laws of the State of .

This Agreement, including the Exhibits, Amendments, and Supplements hereto constitutes the entire Agreement between the parties concerning the subject matter hereof, and shall supersede all previous communications, representations, understandings, and agreements, either oral or written, between the parties.

If any provision of this Agreement is held by any court to be invalid or unenforceable then that provision will be severed from this Agreement and the remaining provisions shall continue in full force.

Article 14

Delivery of Notice. All notices required by this Agreement shall be sufficiently given by mailing the same by certified or registered mail, return receipt requested, to the parties at their respective addresses, as instructed in their (name of applicable document).

Notices to (Escrow Company) should be sent to:

Article 15

Fees. All fees shall be due in full upon the receipt of invoice or at the time of the request for service as the case may be. For the purpose of renewal fees the effective date of this agreement shall be the anniversary date. Fees for services under this agreement shall be paid within 60 days of execution of this Agreement or this Agreement will be automatically terminated. All service fees and renewal fees shall be that specified in (Escrow Company) schedule of fees in effect at the time of renewal, or request for service, except as otherwise agreed. For any increase in (Escrow Company) least 90 days prior to any renewal of this agreement. For any service not listed on the schedule of fees, (Escrow Company) shall provide a quote prior to rendering such service.

(Escrow Company) Vendor

BY BY

(print name) (print name)

TITLE

TITLE

Appendix C

Sample Agreement Between Registered Jurisdiction and Escrow Company

Appendix C

Sample Agreement Between Registered Jurisdiction and Escrow Company

Account Number

This Software Deposit Agreement ("Agreement") is effective this day of , 198 , by and between (Escrow Company) a (State) corporation and ("Purchaser")

WHEREAS, Purchaser has or will enter into a contract(s) with Vendor for the use of computer software and other materials:

WHEREAS, availability of or access to proprietary data related to such computer software and related materials is critical to Registered Jurisdiction in the conduct of its business:

WHEREAS, (Escrow Company) has entered into an agreement with Vendor
pursuant to which (Escrow Company) has agreed to store certain proprietary data relating to the computer software and related materials:

WHEREAS, Vendor has deposited with (Escrow Company) certain proprietary data related to such computer software and related materials:

WHEREAS, Vendor has by a "Registration to Deposit", attached hereto as Exhibit A, designated Registered Jurisdiction to have controlled access to copy of the related proprietary data:

THEREFORE, for good and valuable consideration, the receipt of which is hereby acknowledged, and in consideration of the promises, mutual covenants and conditions contained herein, the parties hereto agree as follows:

Article 1

Definition of Deposit. The Deposit of proprietary data consists of any and all material supplied by Vendor to (Escrow Company) pursuant to the (Agreement between Vendor and Escrow Company) (including amendments thereto), previously entered into between Vendor and (Escrow Company) as specified in the attached

"Description of Deposit Materials."

The Deposit will include any supplemental materials which may be added to the Deposit from time to time by Vendor. (Escrow Company) will notify Registered

Jurisdiction and the Federal Election Commission within ten (10) days of receipt of such supplemental materials.

Article 2

Replacement of Deposit. Vendor may from time to time replace the Deposit with replacement materials. Such replacement Deposit shall be treated by (Escrow Company) as in the case of the initial Deposit. When a Vendor replaces any materials in a Deposit, (Escrow Company) will notify the Registered Jurisdiction and the Federal Election Commission of that replacement. Such notification will be done by mail within ten (10) days of the receipt of the replacement materials by (Escrow Company) .

Article 3

Obligations of (Escrow Company). (Escrow Company) agrees to accept the Deposit referred to in Article 1. (Escrow Company) has establish a receptacle into which it has place the Deposit, and has put the receptacle under the control of one or more officers, selected by (Escrow Company) whose identity shall be available to Registered Jurisdiction at all times. (Escrow Company) will exercise that high level of care in carrying out the terms of this Agreement as (Escrow Company) would use to protect items of this nature which (Escrow Company) might own.

(Escrow Company) shall bear no obligation or responsibility whatsoever to determine the existence, relevance, completeness, currency, accuracy, or any other aspect of the Deposit. (Escrow Company) shall have no obligation or responsibility to determine whether what is deposited is or is not proprietary data as defined or contemplated herein.

Article 4

Term of Agreement. This Agreement shall have an initial term of year(s). This Agreement may be renewed as long as the Vendor's Deposit Agreement is in effect for additional - year periods upon receipt by (Escrow Company) of the specific renewal fee. In the event that the renewal fee is not received on or before the expiration date, Jurisdictions and the Federal Election Commission. A Registered Jurisdiction shall have the right to pay the renewal fee in the event of Vendor's default.

Under no circumstances shall the Federal Election Commission be responsible for any of the fees generated by the Vendor, Vendors, or (Escrow Company) .

Further, the Federal Election Commission is not a party to this Agreement and shall not incur any liability for the actions of the parties involved to this agreement. If the fee is not received within the subsequent thirty (30) days, this Agreement shall expire without further notice and without liability to any other party.

Article 5

Expiry. Upon expiry or non-renewal of this Agreement, all duties and obligations of (Escrow Company) to Registered Jurisdiction hereunder shall terminate. In the event that the Registered Jurisdiction pays the renewal fee and Vendor is of the opinion that any necessary condition for renewal is.not met, Vendor may so notify (Escrow Company) Registered Jurisdiction, and the Federal Election Commission in writing within thirty (30) days of receipt of payment by (Escrow Company) . The resulting dispute shall be resolved pursuant to the Dispute Resolution Process of the "Registration to Deposit Account" (Exhibit A) attached hereto.

Article 6

Delivery of Deposit. In the event that (Escrow Company) is notified by a Registered Jurisdiction of the occurrence of a Release Condition as defined in the "Registration to Deposit" (Exhibit A) along with the payment of the "release request fee" as specified in (Escrow Company) schedule of fees, (Escrow Company) shall so notify Vendor and the Federal Election Commission and shall provide a copy of the notice from the Registered Jurisdiction.

If Vendor provides contrary instructions, as defined in this Article within ten (10) days of the mailing or other service of the notice to Vendor, (Escrow Company) will not deliver a duplicate copy of the Deposit to the Registered Jurisdiction demanding delivery.

If no contrary instructions are received (Escrow Company) will deliver a copy of the Deposit to the Registered Jurisdiction demanding delivery upon payment of (Escrow Company) administrative fees.

Contrary instructions for the purposes of this article means the filing of an affidavit or declaration with (Escrow Company) by Vendor, with a copy to Registered Jurisdiction demanding delivery, and stating that a Release Condition has not occurred, or had been cured. Upon receipt of contrary instructions, (Escrow Company) shall not deliver a copy of the Deposit until otherwise directed by Registered Jurisdiction and Vendor jointly, or until resolution of dispute pursuant to the Dispute Resolution Process defined in the "Registration to Deposit" (Exhibit A) or by a court of competent jurisdiction.

Article 7

Court Orders. If any of the Documentation held in escrow by (Escrow Company) shall be attached, garnished or levied upon pursuant to a court order, or the delivery thereof shall be stayed or enjoined by a court order, or any other order, judgment or decree shall be made or entered by any court affecting the Deposit or any part thereof or any act of (Escrow Company) , (Escrow Company) is hereby expressly authorized in its sole discretion to obey and comply with all orders, judgments or decrees so entered or issued by any court, without the necessity of inquiring whether such court had jurisdiction, and in case (Escrow Company) obeys or complies with any such order, judgment or decree (Escrow Company) shall not be liable to any Registered Jurisdiction, Vendor or any third party by reason of such compliance, notwithstanding that such order, judgment or decree may subsequently be reversed, modified or vacated.

Article 8

Release Conditions. Release conditions shall have the meaning(s) ascribed thereto in the "Registration To Deposit" (Exhibit A) attached hereto.

Article 9

Non-Disclosure. Except as provided in this Agreement, (Escrow Company) agrees that it will not divulge or disclose or otherwise make available to third parties or make any use whatsoever of proprietary information provided to it by Registered Jurisdiction in connection with this Agreement, without the express prior written consent of Registered Jurisdiction. Notwithstanding the above provision, (Escrow Company) shall release the names of Vendor and Registered Jurisdiction(s) to this Agreement to the Federal Election Commission within thirty (30) days of the signing of this Agreement.

Article 10

Indemnification. Vendor agrees to defend and indemnify (Escrow Company) and hold (Escrow Company) harmless from and against any and all claims, actions, and suits, and from and against any and all liabilities, losses, damages, costs, charges, penalties, counsel fees, and other expenses of any nature (including, without limitation, settlement costs) incurred by (Escrow Company) on account of any act or omission of (Escrow Company) in respect to or with regard to this Agreement except as specified in Articles 3 and 9.

Article 11

Audit Rights. (Escrow Company) agrees to keep complete written records

of the activities undertaken pursuant to this Agreement. Registered Jurisdiction shall be entitled at reasonable times during normal business hours and upon reasonable

notice to (Escrow Company) to inspect the records of (Escrow Company)
with respect to this Agreement.

Article 12

Designated Representative. Registered Jurisdiction agrees to designate an authorized individual to receive notices and otherwise act on behalf of Registered Jurisdiction with respect to the performance of its obligations under this Agreement.

Article 13

General. (Escrow Company) may act in reliance upon any instruction,

instrument, or signature believed to be genuine and may assume that any person purporting to give any writing, notice, request, advice or instruction in connection with or relating to this Agreement has been duly authorized to do so.

This agreement shall be governed by, and construed in accordance with the laws

of the State of

This Agreement, including the Exhibits hereto constitutes the entire Agreement between the parties concerning the subject matter hereof, and shall supersede all previous communications, representations, understandings, and agreements, either

oral or written, between the parties.

If any provision of this Agreement is held by any court to be invalid or unenforceable then that provision will be severed from this Agreement and the remaining provisions shall continue in full force.

Article 14

Notice. All notices required by this Agreement shall be sufficiently given by mailing the same by certified or registered mail, return receipt requested, to the parties at their respective addresses, as instructed in the (Name of Applicable Document). Notices to (Escrow Company) should be sent to:

Article 15

Fees. All fees shall be due in full upon the receipt of invoice or at the time of the request for service as the case may be. For the purpose of renewal fees the effective date of this agreement shall be the anniversary date. Fees for services under this agreement shall be paid within 60 days of execution of this agreement or this agreement will be automatically terminated. All service fees and annual renewal fees shall be that specified in (Escrow Company) schedule of fees in effect at the time of renewal, or request for service, except as otherwise agreed. For any increase in (Escrow Company) least 90 days prior to any renewal of this agreement.

For any service not listed on the schedule of fees, (Escrow Company) shall provide a quote prior to rendering such service.

(Escrow Company) Vendor

BY BY

(print name) (print name)

TITLE TITLE

Appendix D

Sample Voting System Procurement Contract Clauses for System Escrow

Appendix D

Sample Voting System Procurement Contract Clauses for System Escrow

The following documents are examples of purchase or lease agreement provisions covering the escrow of source code and related proprietary documentation. The parties may wish to modify the agreements to use among themselves. It is urged that the parties to the agreement each seek legal advice before entering into any agreement to ensure that the individual needs have been satisfied.

Example One

This clause would apply where the documentation is deposited into escrow either before the signing of the purchase or lease agreement or simultaneously with the signing of the purchase or lease agreement.

, Vendor and , Subscriber, hereby agree that Vendor has deposited the items listed on page of Exhibit (entitled) incorporated herein by reference, into escrow with (Name of Escrow Company), located in (City), (State).

Example Two

This Clause is an example of a clause that could be used when the purchase or lease agreement has not yet been signed.

, Vendor and , Subscriber, hereby agree that Vendor will deposit the items listed on page of Exhibit (entitled) incorporated herein by reference, into escrow with (Name of Escrow Company), located in (City), (State). The items referred to above will be deposited within thirty (30) days of the signing of this contract; however, this contract will not come into full effect until the above mentioned items have been deposited and Purchaser receives notification from (Name of Escrow Company) of the deposit.

Appendix E

Sample Supporting Attachments to Escrow Agreements

SERVICE AGREEMENT

This agreement (upon acceptance by [Escrow Company]) initiates the process

of establishing a Software Escrow account. This service agreement does not by itself constitute a Software Escrow account. The current set-up fee is a one-time charge of

$.

(Escrow Company) recognizes the proprietary and confidential rights of

the other parties with respect to this service agreement, the various Agreements between the parties, and all information and materials comprising or representing the Product and Documentation, and will not disclose or use the described information or materials, other than for the purposes for which it is provided.

Responsible Party desires to establish a Software Escrow account for the following computer software or related product material:

Deposit Name

Version Date:

Owner/Developer
Licensor Name

Address

Contract:

Phone: ( )

Check Appropriate: Set-up Free Enclosed

Bill Me

Responsible Party:

Signature Company

Name
Mailing Address

Title

( )
Phone Number City, State, Zip

Accepted By:

Signature Title
Date

SOR

Exhibit A

REGISTRATION TO DEPOSIT ACCOUNT

1. (Seller) (Licensor) has established a Software Deposit Agreement with (Escrow Company) .

2. Licensor hereby designates the following as a Registered Licensee to that Deposit of Proprietary Data described in the Description of Deposited Materials (Exhibit B) to that Software Deposit Agreement:

Jurisdiction Name:
(Buyer)

Mailing Address:

Attention:

Phone: ( )

3. Licensor grants to (Escrow Company) the irrevocable right to copy or reproduce at such time and in such manner as (Escrow Company) in its sole direction determines, such deposit as (Escrow Company) may now or in the future have in its possession. (Escrow Company) will exercise this right only in furtherance of the Software Deposit Agreement between Licensor and (Escrow Company) .

4. Licensor, by amendment, hereby incorporates into that Software Deposit Agreement this Exhibit A and the following attached articles for this particular Registered Licensee:

a. Dispute Resolution Process
b. Release Conditions
c. Provision for Verification
d. Retention of Replaced Deposit e. Transfer of Copy Title

Date: Date:

Supplement Number

Licensor

By:

By:

Title:

Title:

REGISTRATION TO DEPOSIT ACCOUNT

Supplement Number to Account Number

Article

Dispute Resolution Process

Disputes. In the event of a dispute as to which this Article applies, (Escrow Company) shall so notify Licensor and Registered Licensee in writing. Within five business days thereafter, each of Licensor, Registered Licensee, and (Escrow Company) shall designate one referee, who need not be an employee of the designating party. If any party fails within that time to inform the other parties in writing of its designation, the remaining referees may proceed to act in accordance with this Article. Within ten business days after the original notice from (Escrow Company) the referees shall meet and shall entertain such presentation of testimony and other evidence as Licensor and Registered Licensee may wish to present with respect to the dispute. Within five business days after the close of such presentation, the referees shall by majority vote resolve the dispute. The procedure of this Article shall be the exclusive means for resolving disputes to which it applies, and that the decision of the referees shall be final and conclusive. All costs of the referees shall be borne by the unsuccessful party, provided that all costs to (Escrow Company) shall be paid prior to rendering of the referees' decision.

Licensor (Escrow Company)

Initial Initial

REGISTRATION TO DEPOSIT ACCOUNT

Supplement Number to Account Number

Article

Definition of Release Conditions

Release Conditions. The term "release conditions" is defined and used to mean:

1. Failure of Licensor to carry out maintenance or support obligations imposed on it pursuant to the license agreement or other agreement between Licensor and Registered Licensee;

2. Failure of Licensor to continue to do business in the ordinary course;
3. Existence of any one or more of the following circumstances, uncorrected for more than thirty (30) days: entry of an order for relief under Title 11 of the United States Code; the making by Licensor of a general assignment for the benefit of creditors; the appointment of a general receiver or trustee in bankruptcy of Licensor's business or property; or action by Licensor under

   any state insolvency or similar law for the purpose of its bankruptcy, reorganization, or liquidation. The occurrence of the described events shall not constitute a Release Condition, if, within the specified thirty (30) day period, Licensor (including its receiver or trustee in bankruptcy) provides to Registered Licensee adequate assurances, reasonably acceptable to

   Registered Licensee, of its continuing ability and willingness to fulfill all of its maintenance and support obligations.

   (Other release conditions which the parties agree upon should be included in this document)

Licensor (Escrow Company)

Initial Initial

REGISTRATION TO DEPOSIT ACCOUNT

Supplement Number to Account Number

Article

Provision for Verification

Verification and Duplication Rights. In the event that Registered Licensee has separately contracted with (Escrow Company) for additional verification by (Escrow Company) of the Deposit, Licensor hereby grants (Escrow Company) the right to use the facilities of Licensor including without limitation its computer systems and shall make available technical and support personnel necessary for (Escrow Company) to perform such verification.

Licensor (Escrow Company)

Initial Initial

REGISTRATION TO DEPOSIT ACCOUNT

Supplement Number to Account Number

Article

Retention of Replaced Deposit

Retention of Replaced Deposit. Registered Licensee has 20 days from the mailing of notice by (Escrow Company) of the Licensor's replacement of the Deposit with replacement materials, to instruct (Escrow Company) t Replaced Deposit is to be retained. A retention of the replaced deposit by (Escrow Company) will incur an additional fee as specified from time to time by (Escrow Company) schedule of fees. If Registered Licensee does not instruct (Escrow Company) to retain the replaced Deposit, (Escrow Company) will, at Licensor's option, either destroy or return to Licensor such replaced Deposit.

Permission is hereby given by Licensor to (Escrow Company) to retain such replaced deposit if so requested by this Registered Licensee.

Licensor (Escrow Company)

Initial Initial

JURISDICTION SUBSCRIPTION DOCUMENT

Establishing a Subscription

to the Deposit Agreement

Account Number

WHEREAS, Vendor has deposited proprietary data with (Escrow Company) to provide for retention and controlled access for certain Jurisdictions under certain conditions:

(Vendor) addends the Deposit Agreement between Registered Jurisdiction and (Escrow Company) to include the following:

Definition of Subscribed Jurisdiction: Vendor may enroll certain persons, corporations or other legal entities that have entered into an agreement with Vendor regarding the use of Vendor's technology as Subscribed Jurisdictions to this Agreement.

Release of Deposit Copy to Subscribed Jurisdiction: Vendor will instruct and authorize (Escrow Company) to release a copy of the Deposit to an individual Subscribed Jurisdiction upon the payment to (Escrow Company) of the administrative fees for copy and shipping of the Deposit.

Obligations of (Escrow Company) to a Subscribed Jurisdiction: (Escrow Company) is obligated to inform Jurisdiction by regular mail, of their existence as a Subscribed

Jurisdiction to the Deposit agreement. (Escrow Company) is further obligated to

inform Subscribed Jurisdiction of their termination as a Subscribed Jurisdiction to

this Deposit Agreement.

Subscribed Jurisdiction may not request Escrow Company to:

a) continue or stop termination of their Subscribed Jurisdiction status; b) add or change any escrow condition as described above;
c) have any provision for verification of the deposit; and
c) retain an existing deposit.

(Escrow Company) Registered Jurisdiction

Signature	Signature
Title:	Title:
Date:	Date:

SUBSCRIPTION DOCUMENT

Establishing a Subscription Account

to the Deposit Agreement

Account Number

WHEREAS, Vendor has deposited proprietary data with (Escrow Company) to provide for retention and controlled access for certain Jurisdictions under certain conditions:

(Vendor) addends the Deposit Agreement between Vendor and (Escrow Company) to include the following:

Definition of Subscribed Jurisdiction: Vendor may enroll certain Jurisdictions that have entered into an agreement with Vendor regarding the use of Vendor's technology as Subscriber Jurisdictions to this Agreement.

Release of Deposit Copy to Subscribed Jurisdiction: Vendor authorizes (Escrow Company) to release a copy of the Deposit to an Subscribed Jurisdiction upon the payment to (Escrow Company) of the administrative fees for copying and shipping of the Deposit, if and only if, (Escrow Company) has released a copy of the deposit to the state election organization that the Subscriber Jurisdiction resides in.

Obligations of (Escrow Company) to a Subscribed Jurisdiction: (Escrow Company) is obligated to inform Subscriber Jurisdiction by regular mail, of their existence as a Subscribed Jurisdiction to the Deposit Agreement. (Escrow Company) is further

obligated to inform a Subscriber Jurisdiction of their termination as a Subscriber Jurisdiction to this Deposit Agreement.

(Escrow Company) Vendor

Signature	Signature
Title:	Title:
Date:	Date:

ENROLLMENT OF SUBSCRIBED JURISDICTION(S)

Account Number

(Licensor) pursuant to the Deposit Agreement and the Jurisdiction Subscription Document enrolls the following listed Jurisdictions of the Licensor as Subscribed Jurisdictions:

1. Jurisdiction Name

Attention:

Address:

Phone: ( )

2. Jurisdiction Name

Attention:

Address:

Phone: ( )

3. Jurisdiction Name

Attention:

Address:

Phone: ( )

(Escrow Company)

Licensor

Signature	Signature
Title:	Title:
Date:	Date:

Exhibit B

DESCRIPTION OF DEPOSIT MATERIALS

Deposit Account Number

Deposit Account Name

Vendor, persuant to a Deposit Agreement, hereby deposits the below described materials into the above referenced Deposit Account by transferring them to (Escrow Company) . The Deposit Type is: (check box that applies)

Initial Deposit Supplemental Replacement

If no Deposit Type has been checked the materials will be deemed to be an Initial or Supplemental Deposit.

DEPOSIT MATERIALS

Name Version

Date	CPU/OS	Compiler
	Application	
	Utilities needed	
	Special operating instructions	

Item Description Media Quantity

I certify that the above described materials were delivered/sent to (Escrow Company) .Received the materials.

By By
Name Name
Title Title

For	For
(Escrow Company)	
Date	Date

EXHIBIT B NO.

Definitions

Vendor may Update the Deposit Account with Supplemental Materials or Replacement Materials.

Supplemental Materials are materials that are to be added to the existing Deposits by Vendor. The Supplemental Materials will be incorporated into the existing Deposit and treated as the whole.

Replacement Materials are materials that replace the entire deposit materials. Vendor may request to replace the entire existing deposit. The Existing Deposit materials on deposit that have been contractually allowed to be replaced will be dealt with as specified in the Registration to Deposit Agreement, Exhibit A, or by the payment of approapriate update fees.

(Escrow Company) reserves the right to destroy the existing deposit for which of deposit fees have not been paid. (Escrow Company) will notify Vendor of such action.

Warranty by Vendor

Vendor represents and warrants that it is lawfully possessed of all Deposit Materials stored under the Registration to Deposit Agreement and has the authority to store them in accordance with the terms thereof.

Obligations of Escrow Company

To hold these Deposit Materials and treat them as called for in the Registration to Deposit Agreement. If there is no Registration to Deposit Agreement then to not disclose, divulge not otherwise make available to any third party the deposited materials except pursuant to an agreement between Vendor and (Escrow Company) or under the compulsion of a valid court order.

Amendment

This form acts as an Amendment, if one is called for.

•

1. INTRODUCTION

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.

The Federal Election Commission does not intend that these standards restrict the freedom of designers to develop innovative alternatives to current practices. 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. Prior to system qualification, vendors must submit to the test authority certification of compliance with other required federal standards.

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 should prepare design requirements and specifications for the new system, that conform to the functional requirements and performance levels established by the standards.

These specifications should be submitted to the Federal Election Commission (FEC) for review. During product development, the vendor should also submit the Technical Data Package (see Appendix B) to the FEC. The Commission will 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 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.

Source code inspection will involve an evaluation of the software logical correctness, its modularity and the construction, and the extent to which the attributes of simplicity, understandability, testability, robustness, security, usability, installability, maintainability, and modifiability have been incorporated.

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 is required as specified in Sections 7 and 8. Installation of a software package on different hardware than that used during qualification or acceptance testing will require a similar review. This review will determine whether the system must be resubmitted for additional testing.

1.3 Documentation

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

Required records of hardware and software configuration management are described

in Subsections 3.1.1 and 4.3. Records of the quality assurance program are discussed in Section 6. Technical data necessary to conduct the Physical and Functional Configuration Audits are listed in Subsections 7.5.1.2 and 7.5.2.2. A description of the Technical Data Package that is to be provided to the test authority as a precondition of qualification is presented in Appendix B.

1.4 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.

1.4.1 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.

1.4.2 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.

1.4.3 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 electrooptical devices that can be actuated by the voter, that processes the data by means of a computer program, and that records voting data or an electronic image of the ballot in internal memory devices. It produces a tabulation of the voting data at the individual machine level, as hard copy, or stored in a removable memory device.

1.4.4 Subsystems

All voting systems consist of subsystems which are identified by the functions they perform. They are 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 is resident in the voting device (in DRE systems) or ballot-counting device (in P&M systems). It 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 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; the Reporting Subsystem, which consists of hardware and software required to display status reports and messages while the polling place is open, 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 reprocessed data, and other data from external sources to produce the official statement of the vote.

•

A PROCESS FOR EVALUATING

INDEPENDENT TEST AUTHORITIES

FEDERAL ELECTION COMMISSION JANUARY 1990

TABLE OF CONTENTS

Page

A PROCESS FOR EVALUATING INDEPENDENT TEST AUTHORITIES

1.0 Introduction

The role of independent test authorities in the implementation of the Federal Election Commission (FEC) voting systems standards is a crucial one. Test authorities will make the initial determination of voting system compliance with the voluntary standards, and will judge the systems' accuracy, security, and reliability. Therefore, a test authority's expertise and impartiality are vital factors. It is important, then, that vendors choose independent test authorities (ITAs) competent to conduct qualification tests of their voting systems.

It is also important that state and local election officials consider the selected test authority to be credible so that they will not demand repeated qualification testing. This can best be achieved if a national authority provides an objective evaluation of test authorities to aid vendors in their selection.

Because a federally assisted evaluation process is not possible without both Congressional appropriation of necessary funds and time to develop evaluation criteria, some method must be used to identify potential independent test authorities (ITAs) in the interim. In order not to delay issuance and state implementation of the voting systems standards, this plan is being released with short and long term recommendations for this effort. If a formal federal evaluation process is not established, vendors at least will need criteria to assist them in selecting ITAs that are both competent and acceptable to states.

The proposed evaluation process will not only assist vendors in identifying test authorities most capable of testing systems. It will also promote greater uniformity and stability among test authorities and reduce the possibility of repeated qualification testing of voting systems. States will be more certain that tests of voting systems have been executed according to a baseline set of national standards. States may, therefore, be less likely to require vendors to submit their voting systems to duplicate and expensive tests during state certification.

Throughout this process, the FEC will attempt to enlarge the pool of available test authorities willing and able to conduct qualifications tests. To date, only a limited number of organizations have expressed an interest in conducting qualification testing because of the complexities involved.

2.0 The Need For A National Program

States could adopt their own individual ITA evaluation programs. This option, however, would seem very costly and repetitive. Fifty separate assessment procedures would result in a needless duplication of effort. Numerous bodies of this nature, whether informal or otherwise, would also be tremendously cumbersome. Nor is coordination even among small groups of states very likely owing to the oftentimes varied and unique political circumstances within each state. It is also likely that all states would not as readily accept test results from test laboratories evaluated in this manner.

The FEC explored private and public sector alternatives for resolving the issue of a centralized ITA evaluation process and sought the opinions of vendors and state election officials. Respondents overwhelmingly recommended that the process be coordinated by an independent and unbiased third party and, for reasons of credibility, they rejected private associations in favor of a federal agency that would be responsible for the evaluation process.

The FEC subsequently approached the National Voluntary Laboratory Accreditation Program of the National Institute of Standards and Technology (NVLAP/NIST), which is the federal agency experienced in laboratory accreditation and statutorily authorized to perform such formal assessments. NVLAP/NIST agreed to be of some assistance to the FEC in establishing broad assessment criteria that may be employed by voting system vendors in their selection of test authorities. (This segment of the program is hereafter referred to as Phase I.)

Should further funds be available through Congressional appropriations and/or private foundation grants, NVLAP/NIST would build on this criteria to establish a formal ITA accreditation program (Phase II). A NVLAP accreditation program would assess the test authority's internal quality control procedures, test facilities and equipment, key personnel, and knowledge of and experience with appropriate test procedures by means of a formal application and review process. Applicants would be required to certify that no conflict of interest exists between them and any voting system vendor. Technical experts would then evaluate potential test authorities in accordance with the technical criteria through: information supplied by the ITAs in their application, the results of the proficiency tests, and on-site visits. Vendors could then select a test authority from among those that have received NVLAP accreditation.

Neither the vendor-applied ITA evaluation criteria nor the more formal NVLAP accreditation program can guarantee that work performed by approved test authorities will be error free. They can, however, provide some assurance that the chosen ITAs are regarded as capable of adequately testing voting systems and that there is no apparent conflict of interest.

3.0 Interim Selection Of Test Authorities

Until and unless a formal NVLAP accreditation process is established, the FEC recommends that vendors submit their voting systems to one of the major accounting/consulting firms or universities generally recognized across the country as competent in evaluating computer systems. This vendor selection process might be undertaken in coordination with various states.

Local firms or organizations are not recommended in the interim because their lack of instant recognition and credibility among the various states might increase the likelihood that certain states might not accept their test plan and results without duplicative certification testing. Such rejection would either exclude that vendor from subsequent competition or compel a costly re-testing for voting system qualification by a test authority recognized by that state.

To buttress this key element of credibility, it is recommended that vendors select organizations that are clearly independent, that have performed system audits and tests as a third party authority in the past, and that either possess or have access to the technical personnel and full range of facilities and equipment needed to evaluate the systems under the published standards.

Qualification testing of a single voting system may be performed by one test authority, but may also be conducted by different testing bodies that specialize in different aspects of hardware and software evaluation. Whenever more than one organization is involved in qualifying a voting system, the FEC recommends that voting system vendors ensure that a single test authority assume the role of coordinator. This prime contractor should create the test plan, subcontract appropriate tests, collect the test results, and prepare the final report consolidating the test results and presenting the overall system assessment. The prime contractor should also assume full responsibility for the independence and competence of all subcontractors.

The FEC, if Phase I is completed, will recommend criteria that vendors may use to evaluate these nationally recognized, potential test authorities. It is expected that draft criteria will be issued by August 1990. If an accreditation program is established in Phase II, vendors may then select from any accredited test authority.

The FEC's National Clearinghouse on Election Administration (FEC Clearinghouse) will maintain a list of test authorities interested in conducting qualification tests. If Phase II is completed, a list of those accredited by NVLAP will also be available through the FEC Clearinghouse.

4.0 Phase I - Initial Development of Evaluation Criteria

During the proposed Phase I, the FEC will develop an overall plan and, with NVLAP/NIST assistance, identify technical experts representing both government and private sector interests. The technical experts will develop baseline technical evaluation criteria in consultation with NVLAP/NIST and the FEC. While this developmental process is underway, the FEC will contact potential ITAs in an effort to expand the field of those interested in conducting voting system qualification testing.

Prospective ITAs and voting system vendors will be involved in the formulation of the technical criteria. The proposed guidelines will be discussed in public session and drafts will be made available for public comment before they are formally issued to voting system vendors for their use. The FEC will also provide copies of the guidelines to states for informational purposes. The following lists specific tasks that are anticipated during this phase, along with the division of responsibilities among the participants:

ACTION	RESPONSIBILITY
Develop overall plan	FEC
Interact with and inform potential ITAs	FEC
Identify Technical Experts (TEs)	FEC and NVLAP/NIST
Develop technical evaluation criteria based on standards	TEs, NVLAP/NIST, and FEC
Forward evaluation guidelines to voting system vendors and states	FEC
Apply criteria to ITAs	Vendors

The FEC and NVLAP/NIST will avoid recommending evaluation criteria so rigorous as to unduly restrict completion. Because the services to be provided by the independent test authorities are vital to the success of the FEC standards, it is essential that at least a minimum number of approved test authorities remain in operation and that the market is always open for new entrants.

Some preliminary requirements can be specified at this time. First, ITAs must be independent of voting system vendors. They must also be capable of designing, conducting, and reporting the results of qualification tests for different types of computerized voting systems. (See Appendix A for a description of general laboratory requirements necessary to performing qualification tests.)

Specifically, an ITA should have:

_ expertise in overall test plan design to integrate software, hardware and system-level tests;
_ software engineering and hands-on testing expertise;
_ easy access to a facility capable of supporting the environmental tests; and
_ familiarity with pertinent standards and procedures, such as:

- MIL-STD-810 D and MIL-STD-882;
- NASA 975 and NASA 470;
- thermal surveys;
- environmental stress screening;
- U.L. standard rated parts;
- OSHA safety, electrical, thermal and mechanical hazards;
- DOD-STD-2187 and DOD-STD-2188; and—documentation requirements.

Of these criteria, software engineering expertise will be by far the most difficult to evaluate. The difficulty in determining the qualifications of software engineering or testing organizations is a universal problem due primarily to the fact that there is no widely recognized certification of computer professionals or organizations. For although most states issue certificates to "Professional Engineers," these generally apply to electrical and civil engineers rather than software engineers or testers. And while the Institute for the Certification of Computer Professionals offers several levels of certification, these certificates are not widely recognized.

The costs of this phase are difficult to estimate specifically because the evaluation of software testing expertise is a relatively new field. Yet, the FEC envisions that further selection criteria may be established by August 1990.

5.0 Phase II - NVLAP Accreditation

During the proposed Phase II, NVLAP will build upon the work accomplished in Phase

I, assisted by the technical experts. The technical criteria developed in Phase I will be analyzed by NVLAP specialists and refined to provide more elaborate or in-depth qualitative assessment measures. For example, criteria in Phase I might specify that applicants have existing quality control procedures for system testing and written documentation of such procedures. Phase II technical criteria might additionally specify particular characteristics of the required quality control program. In the case of testing expertise, Phase II criteria might specify the number of years experience in various aspects of code analysis, performance testing, and so forth.

The scope of the technical accreditation criteria will be dependent on both time and available funds. If criteria were to be developed to cover assessment of expertise in all test areas (i.e.; electromechanical, safety, quality assurance, software logic and accuracy, and vote count integrity), there would likely be an eighteen to twenty-four month time interval before the first ITA could be accredited. Accordingly, NVLAP proposes an incremental approach whereby Phase I assessment criteria would be employed as broad spectrum indicia. Then, with a shorter time interval of six to eight months, detailed technical criteria can be established in key areas, such as software code analysis for logical correctness and accuracy. After development of these "narrow" criteria, actual accreditation limited to this critical area

could proceed. Depending on the availability of funds, additional criteria could be similarly established and integrated with successive accreditation and periodic ITA review processes.

At the same time as the assessment criteria is being developed, NVLAP personnel and technical experts will develop related ITA proficiency testing programs. These programs provide a formal mechanism for NVLAP off-site assessment of the ITA's hands-on testing capabilities. Heretofore, these programs have included a sample series of step-by step tests, with known results. A laboratory seeking accreditation is required to carry out these proficiency tests as part of the accreditation or periodic review processes.

The duties that are anticipated during this phase are listed below, along with those responsible for performing them. This list includes tasks normally performed during a standard NVLAP accreditation program. It is recognized, however, that these functions may need to be modified in scope to correspond to the voting systems standards testing program. All such functions would be critically assessed prior to the actual accreditation process.

ACTION	RESPONSIBILITY
Provide monetary and in-kind resources to NVLAP/NIST for accreditation program	FEC
Review ITA approval process	TEs and NVLAP/NIST
Refine and detail evaluation criteria	TEs and NVLAP/NIST
Contract with Technical Experts (TEs)	NVLAP
Develop proficiency testing program	TEs and NVLAP/NIST
Interact with and inform laboratories (ITAs)	NVLAP
Review test authority applications	NVLAP
Conduct on-site visits	TEs
Report findings to NVLAP	TEs
Review on-site and proficiency test results	NVLAP/NIST Accredit successful applicants NVLAP/NIST

Although Congressional appropriations and private foundation grants are needed to develop the detailed protocols that would be used in NVLAP accreditation, the program should be virtually self-sufficient once the criteria and proficiency tests are established. Applicants for accreditation would pay a fee which would cover the costs of administering the program.

5.1 Applications For Accreditation

An application would be sent by NVLAP to any test authority on request. The necessary forms, would have to be completed and signed by the organization s authorized representative. Test authorities would be required to designate one individual to perform this function. Although others might be involved in completing the application, the authorized representative would be the only one empowered to alter the scope or nature of the application.

The application for NVLAP accreditation might request:

_ a certification that there is no conflict of interest with any voting system vendor;
_ a description of relevant facilities;

_ a description of relevant testing expertise and capabilities in test plan design;
_ organizational qualifications and experience;

_ related experience, qualifications, and resumes of key support personnel; and

_ estimated time frames for completing various aspects of qualification tests, as specified in the federal standards.

Decisions would be made on the basis of information provided in the application, supporting materials documenting personnel expertise and facilities, and an on-site visit. Experience in conducting comparable examinations and the general approach taken toward software testing and test plan design would also be considered.

5.2 On-Site Assessments

On-site assessments of ITAs may be conducted by one or more technical experts based on a predetermined set of criteria. During an on-site visit to a facility, the evaluators might:

_ inspect the physical plant and the equipment available for testing voting systems;
_ examine the quality assurance measures employed by the test authority;
_ review records of internal audits;
_ evaluate prior experience and expertise in software evaluation of those persons likely to be involved in the testing; and
_ observe software testing methods and techniques.

5.3 Continuing Approval

Test authorities that receive NVLAP accreditation would be subject to periodic review. NVLAP accreditation would also have to be reevaluated in the event that the independent test authority loses or replaces key personnel, files for bankruptcy, is subject to a reorganization, or merges with another company. Accreditation would be suspended if a serious problem is discovered. If NVLAP accreditation were granted and subsequently revoked, the ITA would have to return the accreditation certificate to NVLAP.

5.4 Failure to Receive Approval or Accreditation

A test authority that fails to receive accreditation would be permitted to implement changes as described by NVLAP/NIST in its deficiency notification. In some cases, this might involve only providing NVLAP with additional documentation.

A thirty day notification period is likely in which time the applicant would be asked to respond in writing to the deficiency notification. The ITA would be required to include in this correspondence a plan for correcting these deficiencies or a notification that corrections have been made.

5.5 Compliance With Existing Laws

NVLAP/NIST accreditation would not relieve the test authority from complying with existing Federal, State, or local laws.

APPENDIX A

General Laboratory Requirements for Performing Qualification Tests of Voting Systems

A.1 A Summary of Qualification Tests

Required by the Standards
The Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems segment the qualification tests into three components: hardware tests, software tests, and system-level tests. The hardware and software tests and relevant test specifications are contained in Section 7 (Qualification Test and Measurement Procedures), and Appendices B, and F through 1 (Technical Data

Package, Qualification and Acceptance Test Design, Voting System Failure Definition and Scoring Criteria Qualification Test Plan, and Qualification Test Report.)
The hardware tests consist of both non-operating environmental tests and operating environmental tests. The "non-operating" environmental tests are designed to evaluate the system's ability to withstand storage in the manufacturer's or purchaser's warehouse and transportation associated with delivering the unit to the purchaser or polling place. These tests consist of subjecting the system to environmental conditions such as sudden impact, vibrations, high temperature, low temperature, humidity, and optional rain, and sand and dust exposure. Military laboratories are likely to be equipped to handle these types of tests.

The operating environmental tests are designed to assess the hardware's reliability and accuracy. These tests consist of operating the system for an extended period of time at various temperatures and power voltages that might be encountered during normal operation.

Software evaluation involves the review of documentation for sufficiency, a selectively in-depth examination of source code for design and logical correctness, and the conduct of operational tests to exercise all system functions controlled by the software.

The system-level tests consist of a Functional Configuration Audit and a Physical Configuration Audit. The Functional Configuration Audit determines whether or not the system hardware and software functions as described in the documentation furnished by the system's designer or vendor. This requires conducting tests to assess system performance during the full range of system operations in both normal and abnormal situations induced by the test authority.

The Physical Configuration Audit requires that the system's hardware and software be audited against the vendor's technical documentation in order to establish a baseline for each. Once established, this baseline serves as the reference point for identifying and verifying any subsequent changes (planned or unplanned, accidental or intentional) to the software or hardware.

A.2 General Requirements for Conducting Qualification Tests

The non-operating environmental tests require equipment to measure sudden impact, vibrating platforms, an environmental chamber capable of attaining the required temperatures and humidity, blowing sand and dust chambers, etc. Although these facilities are extensive, the Department of Defense requirements for environmental testing have fostered a number of national laboratories, such as Wyle Laboratories and Viking Laboratories, which are equipped to perform them. Furthermore, the calibration of the equipment in these laboratories is traceable to the National Institute for Standards and Technology by report and date. Although both operating and nonoperating hardware tests require that the independent test authority be familiar with some federal standards and various other military and commercial tests, the "nonoperating" tests do not require the agency performing them to have detailed knowledge of the election process.

The less stringent physical requirements of the operating environmental test can be duplicated in any well equipped industrial or university laboratory. Electrical engineering expertise is required to support these tests and to develop the baseline for the hardware in the Physical Configuration Audit.

The software tests require the independent test authority to examine and evaluate the design and logical correctness of program code and sufficiency of documentation. This task requires expertise in software engineering, including knowledge of the particular computer languages used to program the system.

The software functional tests and the Functional Configuration Audit require that the ITA be skilled in converting the functions claimed by the vendor and the standard's performance requirements into a series of test scenarios which adequately verify the system's capabilities. To accomplish this, the ITA must possess expertise in the analysis of requirements, in experimental test design, in the preparation of detailed test plans and in the analysis of experimental data. In addition to the quantifiable requirements for system qualification, the ITA will be expected to present a qualitative assessment of the system's overall performance, its suitability for elections use and the ease with which it can be maintained and supported.

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-theshelf 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
© 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;

© 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;

© 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;

© 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 equip-

ment;

(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 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

E X H I B I T 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

Sample Size

Precincts

(Devices)

Number Ballots

Number Marks1

100

75,000

7,500,000300

0

9,300,000600

105,000

10,500,00012 155

116,000

11,625,0002500

128,00
0

12,750,0005000

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.

E X H I B I T 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

Number of

Precincts

Number Ballots

Number Marks2
100

75,000

7,000,000300

9,300,000600

105,000

10,500,0001200

116,000

11,625,0002500

128,000

12,750,0005000

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.

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:

	Cross-grain	With-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.

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.

(4)

With-grain		Cross-grain
0.25 percent max.	0.70 percent max.	

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 _ 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.

	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 _ 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 horizon-

tal 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 right2.750 + .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 right2.750 + .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 machinelanguage 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.

-