United States
Election Assistance
Commission

1225 New York Ave. N.W.
Ste.1100
Washington, DC 20005

Testing and Certification Program Manual 2006

DRAFT

www.eac.gov

Table of Contents

DRAFT

1. Introduction

1.1. Background. The Federal Election Commission adopted the first formal set of voluntary national standards for computer-based voting systems in January 1990. At that time, no national program or organization existed to test and certify such systems to the standards. The National Association of State Election Directors (NASED) stepped up to fill this void in 1994. NASED is an independent, non-governmental organization of state election officials. The organization formed the nation's first national program to test and qualify voting systems to the new Federal standards. The organization worked for over a decade, on a strictly voluntary basis, to help assure the reliability, consistency and accuracy of voting systems fielded in the United States. In late 2002, Congress passed the Help America Vote Act of 2002 (HAVA). HAVA created the U.S. Election Assistance Commission (EAC) and assigned to the EAC the responsibility for both setting voting system standards and providing for the testing and certification of voting systems. This mandate represented the first time the Federal government provided for the voluntary testing and certification of voting systems, nationwide. In response to this HAVA requirement, the EAC has developed the Federal Voting System Testing and Certification Program (Certification Program).

1.2. Authority. HAVA requires that the EAC certify and decertify voting systems. Section 231(a)(1) of HAVA specifically requires the EAC to "… provide for the certification, de-certification and re-certification of voting system hardware and software by accredited laboratories." The EAC has the sole authority to grant certification or withdraw certification at the Federal level. This includes the authority to grant, maintain, extend, suspend and withdraw the right to retain or use any certificates, marks or other indicators of certification.

1.3. Scope. This manual provides the procedural requirements of the EAC Voting System Testing and Certification Program. While participation in the program is voluntary, adherence to the program's procedural requirements is mandatory for participants. The procedural requirements of the manual supersede any prior voting system certification requirements issued by the EAC.

1.4. Purpose. The primary purpose of this program is to provide for the testing and certification of voting systems to specified Federal standards consistent with the requirements of HAVA Section 321(a)(1). However, the program also serves to:

1.4.1. Support state certification programs;

1.4.2. Support local election officials in the areas of acceptance testing and pre-election system verification;

1.4.3. Increase quality control in voting system manufacturing; and

1.4.4. Increase voter confidence in the use of voting systems.

1.5. Manual. This manual is a comprehensive presentation of the EAC Voting System Testing and Certification Program. It is intended to establish all of the program requirements.

DRAFT

1.5.1. <u>Contents</u>. The contents of the manual serve as an overview to the program itself. The manual contains the following chapters:

1.5.1.1. *Manufacturer Registration*. Under the program, manufacturers are required to register with the EAC prior to participation. This registration provides the EAC with needed information and requires the manufacture to agree to the requirements of the Certification Program. This chapter sets out the requirements and procedure for registration.

1.5.1.2. *When Voting Systems Must Be Submitted for Testing and Certification*. All systems must be submitted consistent with this manual before they may receive a certification from the EAC. This chapter discusses the various circumstances that require submission in order to obtain or maintain a certification.

1.5.1.3. *Certification Testing and Review*. Under this program, the testing and review process requires the completion of an application, employment of an EAC accredited laboratory for system testing, and technical analysis of the laboratory test report by the EAC. The result of this process is an Initial Decision on Certification. This chapter discusses the required step for voting system testing and review.

1.5.1.4. *Grant of Certification*. If an initial decision to grant certification is made, the manufacturer must take additional steps before it may be issued a certification. These steps require the Manufacturer to document the performance of a trusted build, the deposit of software into a repository and the creation of system identification tools. This chapter outlines the action that manufacturers must take to receive a certification and its post certification responsibilities.

1.5.1.5. *Denial of Certification*. If an initial decision to deny certification is made, the manufacturer has certain rights and responsibilities under the program. This chapter contains procedures for requesting reconsideration, opportunity to cure defects, and appeal.

1.5.1.6. *Decertification*. Decertification is the process by which the EAC revokes a Certification it previously granted to a voting system. It is an important part of the Certification Program, as it serves to ensure that the requirements of the program are followed and that certified voting systems fielded for use in our Federal elections maintain the same level of quality as those presented for testing. This chapter sets procedures for decertification and explains the manufacturer’s rights and responsibilities during that process.

1.5.1.7. *Quality Monitoring Program*. Under the Certification Program, EAC will implement a quality monitoring process that will help ensure that voting systems certified by the EAC are the same systems sold by manufacturers. The quality monitoring process is a mandatory part of the program and

DRAFT

includes elements such as fielded voting system review, anomaly reporting, and manufacturing site visits. This chapter sets forth the requirements of the Quality Monitoring Program.

1.5.1.8. *Interpretation*. An interpretation is a means by which a registered manufacturer or VSTL may seek clarification on a specific Voluntary Voting System Guideline standard. This chapter outlines the policy, requirements, and procedure for requesting an Interpretation.

1.5.1.9. *Trade Secrets, Confidential Commercial and Personal Information*. Federal law protects certain types of information individuals provided the government from release. This chapter outlines the program's policies, sets procedures and discusses responsibilities associated with the public release of potential protected commercial information.

1.5.2. Maintenance and Revision. This manual sets the procedural requirements for a new Federal program and is expected to be improved and expanded as experience and circumstances dictate. The manual will be reviewed periodically and updated to meet the needs of the EAC, Manufactures, VSTLs, election officials and public policy. The EAC is responsible for revisions of this document. All revisions will be made consistent with Federal law. Substantive input from stakeholders and the public will be sought whenever possible, at the discretion of the agency. Changes in policy requiring immediate implementation will be noticed via policy memorandum and issued to each registered manufacturer. Changes, addendums, or updated versions will also be posted to the EAC website at www.eac.gov.

1.6. Program Methodology. EAC's Voting System Testing and Certification Program is but one part of the overall conformity assessment process that includes companion efforts at the state and local levels.

1.6.1. Federal and State Roles. The process to assure that voting equipment meets the technical requirements is a distributed, cooperative effort of federal, state and local officials in the United States. Working with voting equipment manufacturers these officials each have unique responsibility for assuring that the equipment a voter uses on Election Day meets specific requirements.

1.6.1.1. The EAC testing and certification program plays a vital role in the process. The EAC program has primary responsibility for assuring that system designs meet the foundational requirements for all voting equipment in the US.

1.6.1.2. State officials have responsibility for testing voting systems to ensure that they will support the specific requirements of each individual state. Typically state officials will perform mock elections to confirm that a voting system will perform as intended within the election management process of that particular state.

DRAFT

1.6.1.3. State or local officials are responsible for making the final purchase choice. They are responsible to decide which system offers the best fit and total value for their specific state or local jurisdiction.

1.6.1.4. In addition, state or local officials are also responsible for acceptance testing, to assure that the equipment delivered is identical to the equipment certified on the federal and state level is fully operational and meets the contractual requirements of the purchase.

1.6.1.5. State or local officials perform pre-election logic and accuracy testing to confirm that equipment is operating properly and is unmodified from its certified state.

1.6.2. Conformity Assessment, Generally. Conformity assessment is a system established to ensure that a product or service meets the requirements that apply to it. Many conformity assessment systems exist to protect the quality and assure compliance with requirements of products and services. All conformity assessment systems attempt to answer some simple yet difficult questions:

1.6.2.1. *What specifications are required of an acceptable system*? For voting systems, the EAC voting system standards (VVSG and VSS) address this issue. States and local jurisdiction also have supplementing standards.

1.6.2.2. *How are systems tested against required specifications?* The EAC Voting System Testing and Certification Program is a central element of the larger conformity assessment system. The program, as set forth in this manual, provides for the testing and certification of voting systems to identified versions of the VVSG. The testing and certification program's purpose is to assure that state and local jurisdictions receive voting systems that meet the requirements of the VVSG.

1.6.2.3. *Are the testing authorities qualified to make an accurate evaluation*? The EAC accredits Voting System Testing Laboratories (VSTLs), after the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP) has reviewed their technical competence and lab practices, to ensure these test authorities are fully qualified. Furthermore, EAC technical experts review all test reports from accredited laboratories to ensure accurate and complete evaluation. Many states provide similar reviews of laboratory reports.

1.6.2.4. *Will Manufacturers deliver units within manufacturing tolerances to those tested?* The VVSG and this manual require that vendors have appropriate change management and quality control processes to control the quality and configuration of their products. The Certification Program provides mechanisms for the EAC to verify manufacturer quality processes through

DRAFT

field system testing and manufacturing site visits. States have implemented policies for acceptance of delivered units.

1.7. Program Personnel. All EAC personnel and contractors associated with this program will be held to the highest ethical standards. All agents of the EAC involved in the certification program will be subject to a conflict of interest reporting and review, consistent with Federal law and regulation.

1.8. Program Records. The EAC Program Director is responsible for maintaining accurate records to demonstrate that the testing and certification program procedures have been effectively fulfilled and to ensure the traceability, repeatability, and reproducibility of testing and test report review. All records will be maintained, managed, secured, stored, archived and disposed of in accordance with Federal law, regulation and procedures of the EAC.

1.9. Submission of Documents. Any documents submitted pursuant to the requirements of this manual shall be submitted:

1.9.1. Electronically, either via secure e-mail or physical delivery of CD-ROM, unless otherwise specified;

1.9.2. In an unalterable Microsoft Word or Adobe PDF format.

1.9.3. Using an electronic signature. Documents that require an authorized signature shall be signed with the electronic signature (digitized) of an authorized management representative and must meet any and all subsequent requirements established by the Program Director regarding security.

1.9.4. If via physical delivery, shall be sent by certified mail (or similar means that allow tracking) to:

Testing and Certification Program Director,
U.S. Election Assistance Commission
1225 New York Ave, Suite 1100
Washington, DC 20005

1.10. Receipt of Documents. For the purposes of this manual, a document, notice or other communication is considered received by a manufacturer upon the earlier of:

1.10.1. The actual, documented date the correspondence was received (either electronically or physically) at the manufacturer’s place of business; or

1.10.2. The date of constructive receipt for the communication. For electronic correspondence, documents will be constructively received the day after the date sent. For mail correspondence, document will be constructively received three days after the date sent.

DRAFT

1.10.3. The term receipt shall mean the date a document or correspondence arrived (either electronically or physically) at the Manufacturer's place of business. Arrival does not require that an agent of the manufacturer opened, read or review the correspondence.

1.11. Records Retention. The manufacturer is responsible for ensuring that all documents submitted to the EAC or that otherwise serve as the basis for the certification of a voting system are retained. A copy of all such records shall be retained as long as the voting system is in use or for sale in the United States and for three years thereafter.

1.12. Publication and Release of Documents. The EAC will release documents consistent with the requirements of Federal law. It is EAC policy to make the certification process as open and public as possible. To this end, any documents submitted under this program and not protected from release by law, will be made available to the public. The primary means for making this information available is through the EAC website.

1.13. Definitions. For the purpose of this manual, the terms listed below have the following definitions.

Appeal: A formal process by which the EAC is petitioned to reconsider a final agency decision.

Appeal Authority: The individual or individuals appointed to serve as the determination authority on appeal.

Build Environment: The disk or other media which holds the source code, compiler and other necessary files for the compilation and on which the compiler with store the resulting executable code. A compiler is a computer program that translates programs expressed in a high-order language into their machine language equivalents.

Certificate of Conformance: The certificate issued by the EAC when a system has been found to meet the requirements of the VVSG. The document conveys certification of a system.

Commission: The U.S. Election Assistance Commission, as an agency.

Commissioners: The serving commissioners of the U.S. Election Assistance Commission.

Days: The term days shall refer to calendar days, unless otherwise noted. When counting days, for the purpose of submitting or receiving a document, the count shall begin on the first full calendar day after the day the document was received.

Digital Signature: The signature of a file produced using a HASH algorithm. A digital signature creates a value that is "Computationally infeasible" for two different files less than 264 bits in size produce the same value. Digital signatures are utilized to verify that files are unmodified from their original. For the purposes of this manual, the HASH algorithm shall be the minimum current recommendation of the NIST NSRL, which is currently the Secure Hash Algorithm (SHA-1) specified in FIPS 180-1.

DRAFT

Disk Image: An exact copy of the entire contents of a computer disk.

Election Official: A state or local government employee, who has as one of his or her primary duties the management or administration of a Federal Election.

Federal Election: Any primary, general, run-off or special election in which a candidate for Federal office (President, Senator or Representative) appears on the ballot.

Fielded Voting System: A voting system purchased or leased by a state or local government that is being use in a Federal Election.

Installation Disk: A computer disk containing program files and software to install them onto a computer or other device.

Memorandum for the Record: A written statement drafted to document an event or finding, without a specific addressee other than the pertinent file.

Manufacturer: The entity with ownership and control over a voting system submitted for certification.

Mark of Conformance: A uniform notice permanently posted on a voting system which signifies that it has been certified by the EAC.

Proprietary Information: Commercial information or trade secrets protected from release under the Freedom of Information Act and the Trade Secrets Act.

Receipt (of a document): For the purposes of this manual

Technical Reviewers: Technical experts in the areas of voting system technology and conformity assessment used by the EAC to provide expert guidance.

Testing and Certification Decision Authority: The EAC Executive Director or individual appointed by the Executive Director authorized to make final agency determinations on certification.

Testing and Certification Program Director: The individual appointed by the EAC Executive Director to administer and manage the Testing and Certification Program.

Voting System: The total combination of mechanical, electromechanical and electronic equipment that is used to define ballots; to cast and count votes; to report or display election results; to connect the voting system to the voter registration system; and to maintain and produce any audit trail information.

Voting System Test Laboratories: Laboratories accredited by the EAC to test voting systems to the VVSG, consistent with the requirements of this manual.

DRAFT

Voting System Standards: Voluntary voting system standards developed by the Federal Election Commission. Voting System Standards have been published twice, once in 1990 and again in 2002. The Help America Vote Act made the 2002 Voting System Standards EAC guidance. All new voting system standards are issued by the EAC as Voluntary Voting System Guidelines.

Voluntary Voting System Guidelines: Voluntary voting system standards developed, adopted and published by the EAC. The guidelines are identified by version number and date.

1.14. Acronyms and Abbreviations. For the purpose of this manual, the acronyms and abbreviations listed below represent the following terms.

Certification Program: The EAC Voting System Testing and Certification Program

EAC: United States Election Assistance Commission

Decision Authority: Testing and Certification Decision Authority

HAVA: Help America Vote Act of 2002

Labs or Laboratories: Voting System Test Laboratories

NIST: National Institute of Standards and Technology

NVLAP: National Voluntary Laboratory Accreditation Program

Program Director: Director of the EAC's Testing and Certification Program

VSTL: Voting System Test Laboratory

VSS: Voting System Standards

VVSG: Voluntary Voting System Guidelines

DRAFT

2. Manufacturer Registration

2.1. Overview. Manufacturer Registration is the process by which voting system manufacturers make initial contact with the EAC and provide information essential to participate in the EAC's voting system testing and certification program. Before a manufacturer of a voting system can submit an application to have a voting system certified by the EAC, the vendor must be registered. This process requires the manufacturer to provide certain contact information and agree to certain requirements of the Certification Program. Once successfully registered, the manufacturer will receive an identification code.

2.2. Registration Required. In order to submit a voting system for certification or otherwise participate in the EAC Voluntary Voting System Certification Program, a manufacturer must register with the EAC.

2.3. Registration Requirements. The registration process will require the voting system manufacturer to provide certain information to the EAC. This information is necessary to enable the EAC to administer the Certification program and communicate effectively with the Manufacturer. The registration process also requires the Manufacturer to agree to certain certification program requirements. These requirements deal with some of the manufacturer's duties and responsibilities under the program. In order for this program to succeed it is vital that a manufacturer know and assent to these duties at the outset of the program.

2.3.1. <u>Information</u>. Manufactures are required to provide the following information:

2.3.1.1. The manufacturer's organizational information, including:

2.3.1.1.1. The official name of the manufacturer;

2.3.1.1.2. Address of manufacturer's official place of business;

2.3.1.1.3. A description of how the manufacturer is organized (i.e. type of corporation or partnership);

2.3.1.1.4. Names of officers and/or members of the board of directors;

2.3.1.1.5. Names of any and all partners;

2.3.1.1.6. Identification of any individual, organization or entity with a controlling ownership interest in the manufacturer;

2.3.1.2. The identity of an individual authorized to represent and make binding commitments and management determinations for the Manufacturer (management representative). The information required for the individual includes:

2.3.1.2.1. Name and title;

DRAFT

2.3.1.2.2. Mailing and physical addresses;

2.3.1.2.3. Telephone number, fax number and email address.

2.3.1.3. The identity an individual authorized to provide technical information on behalf of the manufacturer (technical representative). The information required for the individual includes:

2.3.1.3.1. Name and title;

2.3.1.3.2. Mailing and physical addresses;

2.3.1.3.3. Telephone number, fax number and email address

2.3.1.4. The Manufacturer's written policies regarding its quality assurance system. This policy must be consistent with guidance provided in the VVSG and this manual.

2.3.1.5. The Manufacturer's written polices regarding internal procedures for controlling and managing changes to and versions of its voting systems. Such polices shall be consistent with this manual and guidance provided in the VVSG.

2.3.1.6. The Manufacturer's written polices on document retention. Such policies must be consistent with the requirements of this manual.

2.3.1.7. A list of production facilities used by the Manufacturer and the name and contact information of a person at each facility. The information required for each individual, includes:

2.3.1.7.1. Name and title;

2.3.1.7.2. Mailing and physical addresses; and

2.3.1.7.3. Telephone number, fax number and email address.

2.3.2. Agreements. Manufacturers are required to take or abstain from certain actions in order to protect the integrity of the certification program and promote quality assurance. Manufacturers are required to agree to the following program requirements:

2.3.2.1. Represent a voting system as certified only when authorized by the EAC and consistent with the procedures and requirements of this manual.

DRAFT

2.3.2.2. Produce and permanently affix an EAC certification label to all production units of the certified system. Such labels must meet the requirements put forth in Chapter 5.

2.3.2.3. Notify the EAC of changes to any system previously certified by the EAC pursuant to the requirements of this Manual (see Chapter 3). Such systems shall be submitted for testing and additional certification when required.

2.3.2.4. Permit an EAC representative to verify manufacturer quality control, by cooperation with EAC efforts to test and review fielded voting systems consistent with Section 8.6 of this Manual.

2.3.2.5. Permit an EAC representative to verify manufacturer quality control, by conducting periodic inspections of manufacturing facilities consistent with Chapter 8 of this Manual.

2.3.2.6. Cooperate with any EAC inquiries and investigations into a certified systems compliance with VVSG standards or the procedural requirements of this manual consistent with Chapter 10.

2.3.2.7. Report to the Program Director any known malfunction of a voting system holding an EAC Certification. A malfunction is failure of a voting system, not caused by operator or administrative error, which causes the system to fail or otherwise not operate as designed.

2.3.2.8. Certify that the entity is not bared or otherwise prohibited by statute, regulation or ruling from doing business in the United States.

2.3.2.9. Adhere to all procedural requirements of this Manual.

2.4. Registration Process. Generally, registration is accomplished through use of the EAC registration form. Once a registration form and other required registration documents have been received by the EAC, the information is reviewed for completeness and approved.

2.4.1. Application Process. To become a registered voting system manufacturer, one must apply by submitting a Manufacturer Registration Application Form (Appendix A). This form will be used as the means for the manufacturer to provide the information and agree to the responsibilities required in section 2.3, above.

2.4.1.1. *Application Form*. In order for the EAC to accept and process the registration form:

2.4.1.1.1. All fields must be completed by the manufacturer;

DRAFT

2.4.1.1.2. All required attachments prescribed by the form and this manual are identified, complete and timely forwarded to the EAC (i.e. Manufacturer's quality control and system change policies); and

2.4.1.1.3. The application form is affixed with the signature (including a digital representation of a hand written signature) of the authorized representative of the vendor.

2.4.1.2. *Availability and Use of the Form*. The Manufacturer Registration Application Form may be accessed through the EAC web site at www.eac.gov. Instructions for completing and submitting the form are included on the website. The webs cite will also provide contact information regarding questions about the form or the application process.

2.4.2. EAC Review Process.

2.4.2.1. Once the application form and required attachments have been submitted, the applicant will receive an acknowledgement that the EAC has received the submission and that the application will be processed.

2.4.2.2. If a form is submitted incomplete or an attachment is not provided, the EAC will notify the manufacturer and request the information. Registration applications will not be processed unless they are complete.

2.4.2.3. Upon receipt of the completed registration form and accompanying documentation, the EAC will review the information for sufficiency. If the EAC requires clarification or additional information, the EAC will contact the manufacture and request the needed information.

2.4.2.4. Upon satisfactory completion of a registration application's sufficiency review, the EAC will notify the Manufacturer that it has been registered.

2.5. Registered Manufacturers. Once a manufacturer has received notice that it is registered, it will receive an identification code, password and will be eligible to participate in the voluntary voting system certification program.

2.5.1. Manufacturer Code. Registered manufacturers will be issued a unique, three-letter identification code. This code will be used to identify the manufacturer and its products.

2.5.2. Continuing Responsibility to Report. Registered Manufacturers are required to keep all registration information up-to-date. Manufacturers must submit a revised application form to the EAC within 30 days of any changes to the information required on the

DRAFT

application form. Manufacturers will remain registered participants in the program during this up-date process.

2.5.3. Program Information Updates. Registered manufacturers will be automatically provided timely information relevant to the certification program.

2.5.4. Website Postings. The EAC will add the Manufacturer to the EAC listing of registered voting system Manufacturers publicly available at www.eac.gov.

2.6. Suspension of Registration. Manufacturers are required to establish policies and operate within the EAC certification program consistent with the procedural requirements laid out in this Manual. When manufacturers are engaging in management activities that violate the program's requirements, their registration may be suspended until such time as the problem is remedied.

2.6.1. Procedures. Where a manufacturer's activities violate the procedural requirements of this manual they will be notified of the violations, given an opportunity to respond and provided the steps required to bring themselves into compliance.

2.6.1.1. *Notice*. Manufacturers shall be provided written notice that they have taken action inconsistent with or failed to act in violation of the requirements of this manual. The notice will state the violations and the specific steps required to cure them. The notice will also provide them with 30 days (or a greater period of time as stated by the Program Director) to (1) respond to the notice and/or (2) cure the defect.

2.6.1.2. *Manufacturer Action*. The Manufacturer is required to either timely respond to the notice (demonstrating that it was not in violation of program requirements) or timely cure the violations identified. In any case, Manufacturer action must be approved by the Program Director to prevent suspension.

2.6.1.3. *Non-Compliance*. If the Manufacturer fails to timely respond, is unable to provide a cure or response acceptable the Program Director, or otherwise refuses to cooperate, the Program Director may suspend the Manufacturer's registration. The Program Director shall issue a notice of his or her intent to suspend and provide the Manufacturer five working days to object to the action and submit information in support of the objection.

2.6.1.4. *Suspension*. After notice and opportunity to be heard (consistent with the above), the Program Director may suspend a Manufacturer's registration. The suspension shall be noticed in writing. The notice must inform the Manufacturer of the steps that can be taken to remedy the violations and lift the suspension.

DRAFT

2.6.2. Effect of Suspension. A suspended Manufacturer may not submit a system for certification under this program. A suspension shall remain in effect until lifted. Manufacturers always have the right to remedy a non-compliance and lift a suspension consistent with EAC guidance. Failure of a Manufacturer to follow the requirements of this section may also result in decertification of voting systems consistent with Chapter 7 of this Manual.

DRAFT

3. When Voting Systems Must Be Submitted for Testing and Certification.

3.1. Overview. An EAC Certification signifies that a voting system has been successfully tested to identified, voting system standards adopted by the EAC. Only the EAC can issue a Federal Certification. Ultimately, systems must be submitted for testing and certification under this program to receive this certification. Systems will usually be submitted when (1) they are new to the marketplace, (2) they have never before received an EAC Certification, (3) they are modified and (4) the manufacturer wishes to test a previously certified system to a different (newer) standard.

3.2. What is an EAC Certification? Certification is the process by which the EAC, through testing and evaluation conducted by an accredited Voting System Test Laboratory (VSTL), validates that a voting system meets the requirements set forth in existing voting system testing standards (VSS or VVSG), and performs according to the manufacturer's specifications for the system. An EAC Certification may only be issued by the EAC in accordance with the procedures laid out in this manual. Certifications issued by other bodies (e.g. NASED and state certification programs) are not EAC Certifications.

3.2.1. Types of voting systems certified. The EAC Certification Program is designed to test and certify electromechanical and electronic voting systems. The EAC will not accept for certification review voting systems that do not contain any electronic components. Ultimately, the determination of whether a voting system meets these requirements is a determination of the EAC.

3.2.2. Voting system standards. Voting systems certified under this program are tested to a set of voluntary standards providing requirements that voting systems must meet to receive a Federal Certification. Presently, these standards are referred to as Voluntary Voting System Guidelines (in the past they were called Voting System Standards).

3.2.2.1. *Versions—availability and identification*. Voluntary Voting System Guidelines (or applicable Voting System Standards) are published by the EAC and available on the EAC website (www.eac.gov). The standards will be routinely updated. Versions will be identified by version number and/or release date.

3.2.2.2. *Versions—basis for certification***.** The EAC will promulgate which version or versions of the standards it will accept as the basis for testing and certification. This may be accomplished through the setting of an implementation date for a particular version's applicability or the setting a date by which testing to a particular version is mandatory. The EAC will only certify voting systems tested to standards it has identified as valid for certification.

3.2.2.2.1. End date. When a version's status as the basis of an EAC Certification is set to expire on a date certain, the submission of the system's test report will be the controlling event (See Chapter 4). This means the system's test report must be received by the EAC

DRAFT

on or before the end date to be certified to the terminating standard.

3.2.2.2.2. Start date. When a version's status as the basis of an EAC Certification is set to begin on a date certain, the submission of the system's application for certification will be the controlling event (See Chapter 4). This means the system's application, requesting certification to the new standard, will not be accepted by the EAC until the start date.

3.2.2.3. *Version—manufacturer's option*. When the EAC has authorized certification to more that one version of the standards, the manufacturer must choose which version it wishes to have its voting system tested against. The voting system will then be certified to that version of the standard. Manufacturers must ensure that all applications for certification identify a particular version of the standards.

3.2.2.4. *Emerging technologies*. If a voting system or component thereof is eligible for a certification under this program (see Section 3.2.1.) and employs technology which is not addressed by a presently accepted version of the VVSG or VSS, the system shall be subjected to full integration testing and testing to ensure that it operates to the manufacturer's specifications. Information on emerging technologies will be forwarded to the U.S. Election Assistance Commission's Technical Guidelines Development Committee.

3.2.3. <u>Significance of an EAC Certification</u>. An EAC certification is an official recognition that a voting system (in a specific configuration) has been tested to and met an identified set of Federal voting standards. An EAC Certification is <u>not</u>:

3.2.3.1. an endorsement of a manufacturer, voting system or any of the system's components;

3.2.3.2. a Federal warranty of the voting system or any of its components;

3.2.3.3. a determination that a voting system, when fielded, will meet all HAVA requirements;

3.2.3.4. a substitute for State or local certification and testing;

3.2.3.5. a determination that the system is ready for use in an election; or

3.2.3.6. a determination that any particular component of a certified system is itself certified for use outside the certified configuration.

3.3. Effect of EAC Certification Program on Other National Certifications. Prior to the creation of the EAC Certification Program, national voting system qualification was conducted

DRAFT

by a private membership organization, the National Association of State Election Directors (NASED). NASED offered a qualification for voting systems for over a decade, using standards issued by the Federal government. EAC's certification program does not repeal NASED issued qualifications. All voting systems previously qualified under the NASED program retain their NASED qualification consistent with state law. In any event, a NASED qualified voting system is not EAC Certified and is treated like an uncertified system for the purposes of this program.

3.4. When Certification is Required under the Program. In order to obtain or maintain an EAC Certification, manufacturers must submit a voting system for testing and certification under this program. Such action is usually required for (1) new systems not previously tested to any standard; (2) existing systems not previously certified by the EAC; (3) previously certified systems that have been modified; or (4) previously certified systems which the manufacturer seeks to upgrade to a higher standard (i.e. more recent version of the VVSG).

3.4.1. New System Certification. New systems are defined, for the purposes of this manual, as voting systems which have not been previously tested to applicable Federal standards. New voting systems must be fully tested and submitted to the EAC per the requirements of Chapter 4 of this manual.

3.4.2. Systems not previously EAC Certified. This term describes any voting system not previously certified by the EAC. This includes systems previously tested and qualified by NASED or systems previously test and denied certification by the EAC. Such systems must be fully tested and submitted to the EAC per the requirements of Chapter 4 of this manual.

3.4.3. Modifications. A modification is any change to *a previously EAC Certified voting system's* hardware, software or firmware. Modifications to voting systems will require testing and review by the EAC in accordance with the requirements of Chapter 4 of this manual.

3.4.4. Certification Upgrade. This term defines any system previously certified by the EAC, but submitted for additional testing and certification to a higher standard (i.e. to a newer version of the VVSG). Such systems must be tested to the new standards and submitted to the EAC per Chapter 4 of this manual.

3.5. Provisional, Pre-Election Emergency Modifications. In order to deal with extraordinary, pre-election, emergency situations, the EAC has developed a special provisional modification process. This process is **only** to be used for the emergency situations indicated, and **only** when there is a clear and compelling need for temporary relief until the regular certification process can be followed.

3.5.1. Purpose. The purpose of this section is to allow a mechanism within the EAC Certification Program for manufacturers to modify EAC certified voting systems in emergency situations immediately prior to an election. This situation arises when a modification to a voting system is required and an election deadline is imminent,

DRAFT

preventing the completion of the full certification process (and State and/or local testing process) in time for Election Day. In such situations the EAC may issue a waiver to the manufacturer, granting it leave to make the modification without submission for modification testing and certification.

3.5.2. General Requirements. A request for an emergency modification waiver may only be made by a manufacturer *in conjunction* with the State or local election official whose jurisdiction(s) would be adversely affected if the requested modification were not implemented before Election Day. Requests must be submitted at least five calendar day prior to an election. Only systems previously certified are eligible for such a waiver. To receive a waiver a manufacturer must demonstrate:

3.5.2.1. The modification is functionally or legally required, such that the system cannot be fielded in an election without the change.

3.5.2.2. The voting system requiring modification is need by state or local election officials to conduct a pending Federal election.

3.5.2.3. The voting system to be modified has previously been certified by the EAC.

3.5.2.4. The modification cannot be tested by a VSTL and submitted to the EAC for certification, consistent with the procedural requirements of this manual, at least 30 days before the pending Federal election.

3.5.2.5. Relevant state law requires Federal certification of the requested modification.

3.5.2.6. The manufacturer has taken steps to ensure that the modification will properly function as designed, is suitably integrated with the system and otherwise will not negatively affect system reliability, functionality and accuracy.

3.5.2.7. The Manufacturer has completed as much of the evaluation testing as possible for the modification and has provided the results of such testing to the EAC.

3.5.2.8. The emergency modification is required and otherwise supported by an election official seeking to field the voting system in an impending Federal election.

3.5.3. Request for Waiver. A Manufacturer's request for waiver shall be made in writing to the Decision Authority and shall include:

3.5.3.1. A statement providing sufficient description, background, information, documentation and other evidence necessary to demonstrate that the request for a waiver meets each of the eight requirements stated in section 3.5.2., above.

DRAFT

3.5.3.2. A signed statement from the chief election official in the locality or state which is requiring the emergency modification. This signed statement shall identify the pending election creating the emergency situation and attest that (1) the modification is required to field the system, (2) state law requires EAC action in order to field the system in an election, and (3) normal timelines required under the EAC Certification Program cannot be met.

3.5.3.3. A signed statement from a VSTL that there is insufficient time to perform necessary testing and complete the certification process. The statement shall also state what testing has been performed on the modification to date, provide the results of such tests and state the schedule for completion of testing.

3.5.3.4. A detailed description of the modification, the need for the modification, how it was developed, how it addresses the need for which it was designed, its impact on the voting system, and how the modification will be timely fielded or implemented.

3.5.3.5. Any and all documentation of tests performed on modification by the manufacturer, a laboratory or other third party.

3.5.3.6. A stated agreement signed by the manufacturer's representative agreeing to:

3.5.3.6.1. Submit for testing and certification, consistent with Chapter 4 of this manual, any voting system receiving a waiver under this section which has not already been submitted. This shall be done immediately.

3.5.3.6.2. Abstain from representing the modified system as EAC certified. The modified system has not been certified; rather the originally certified system has received a waiver providing the manufacturer leave to modify it.

3.5.3.6.3. Submit a report to the EAC regarding the performance of the modified voting system within 60 days of the Federal election which served as the basis for the waiver. This report shall identify and describe any (1) performance failures, (2) technical failures, (3) security failures, and/or (4) accuracy problems.

3.5.4. EAC review. EAC will review all waiver requests timely submitted and make determinations regarding the requests. Incomplete requests will be returned for resubmission with a written notification regarding its deficiencies.

3.5.5. Letter of Approval. If the EAC approves the modification waiver, the Decision Authority shall issue a letter granting the temporary waiver.

DRAFT

3.5.6. Effect of Grant of Waiver. An EAC grant of waiver for an emergency modification is not an EAC certification of the modification. Waivers under this program only grant manufacturers leave to temporarily amend previously certified systems without testing and certification for the specific election noted in the request. Without such a waiver, such action would ordinarily result in decertification of the modified system. Systems receiving a waiver shall satisfy any state requirement that a system be nationally or Federally certified. Additionally:

3.5.6.1. All waivers are temporary and expire 60 days after the Federal Election for which the system was modified and waiver granted.

3.5.6.2. Any system granted a waiver must be submitted for testing and certification immediately following the Federal election for which the waiver was granted.

3.5.6.3. The grant of a waiver is no indication that the modified system will ultimately be granted a certification.

3.5.7. Denial of Request for Waiver. A denial of a request for emergency modification by the EAC shall be final and not subject to appeal. Manufacturers may submit for certification, consistent with Chapter 4 of this manual, modifications for which emergency waivers were denied.

DRAFT

4. Certification Testing and Technical Review

4.1. Overview. This chapter discusses the procedural requirements for submitting a voting system to the EAC for testing and review. The testing and review process requires an application, employment of an EAC accredited testing laboratory and technical analysis of the laboratory test report by the EAC. The result of this process is an Initial Decision on Certification by the Decision Authority.

4.2. Policy. Generally, in order to receive an initial determination on an EAC Certification for a voting system, a registered Manufacturer must have (1) submitted an EAC-approved application for certification, (2) submitted an EAC-approved test plan created by an accredited laboratory, (3) tested a voting system to applicable voting system standards using an accredited VSTL, (4) submitted a test report (through the VSTL) to the EAC for technical review and approval and (5) received EAC approval of the report in an Initial Decision on Certification.

4.3. Certification Application. The first step in submitting a voting system for certification is submission of an application package. The Package contains an application form and a copy of the Technical Data Package for the system submitted for testing and certification. The process initiates the certification process and provides the EAC with needed information.

4.3.1. Information. The application (application form) provides certain pieces of information to the EAC which are essential at the outset of the certification process. This information includes:

4.3.1.1. *Manufacturer Information*. Identification of the Manufacturer (name and three letter identification code);

4.3.1.2. *Accredited Laboratory Information*. Identification of the accredited laboratory which will perform voting system testing and other prescribed laboratory action consistent with the requirements of this manual;

4.3.1.3. *Voting System Standards Information*. Identification of the Voluntary Voting System Guidelines or Voting Systems Standards, including the document's date and version number, to which the manufacture wishes to have the identified voting system test and certified;

4.3.1.4. *Nature of the submission*. Manufacturers must identify nature of their submission by selecting one of four submission types:

- New Systems. New systems are defined, for the purposes of this manual, as voting systems which have not been previously tested to any applicable Federal standards.

- Systems not previously EAC Certified. This term describes any voting system not previously certified by the EAC. This includes systems

DRAFT

previously tested and qualified by NASED or systems previously test and denied certification by the EAC.

- Modifications. A modification is any change to *a previously EAC Certified voting system's* hardware, software or firmware.

- Certification Upgrade. This term defines any system previously certified by the EAC, but submitted (without modification) for additional testing and certification to a higher standard (i.e. to a newer version of the VVSG).

4.3.1.5. *Identification of the Voting System*. Manufacturers must identify the system submitted for testing by providing its name and applicable version number. If the system submitted has been previously fielded, but the manufacturer wishes to change its name or version number after receipt of EAC Certification, it must provide identification information on both the past name or names and the new, proposed name. This might occur in systems submitted for modification, for their first EAC certification or for a certification upgrade.

4.3.1.6. *Description of Voting System*. Manufacturers must provide a brief description of the system or modification being submitted for testing and certification. This information shall include:

4.3.1.6.1. A listing of all components of the system submitted,

4.3.1.6.2. Each component's version number,

4.3.1.6.3. Any other information necessary to identify the specific configuration being submitted for certification.

4.3.1.7. *Date submitted*. Manufacturers must note the date the application was submitted for EAC approval.

4.3.1.8. *Signature*. The Manufacturer must affix the signature of the authorized management representative.

4.3.2. Submission of the Application Package. Manufacturers must submit a copy of the application form described above and copies of all relevant Technical Data Packages.

4.3.2.1. *Application Form*. Application forms will be available on EAC's website. The application form submitted to the EAC must be signed, dated and fully, accurately and completely filled out. Incomplete or inaccurate application forms will not be accepted.

4.3.2.2. *Technical Data Package(s)*. The manufacture must submit with the application form a copy of the voting system's technical data package. This

DRAFT

technical data package must meet the requirements of the VVSG. If an existing system is being submitted with a modification, the manufacturer must submit a copy of the revised Technical Data Package. The Manufacturer shall also submit the original data package which served as a basis for the prior EAC certification.

4.3.2.3. *Submission*. Applications and Technical Data Packages shall be submitted in Adobe PDF, Microsoft Word or other electronic formats as prescribed by the Program Director. Information on how to submit packages will be posted on EAC's website.

4.3.3. EAC Review. Upon receipt of a Manufacturer's application package, the EAC will review the submission for completeness and accuracy. If the application package is incomplete, it will be returned to the manufacturer with instructions for resubmission. If the form submitted is acceptable, the manufacturer will be notified and provided a unique application number within five working days of the EAC's receipt of the application.

4.4. Test Plan. The manufacturer shall authorize the accredited lab identified in its application to submit a test plan. This plan shall provide for testing of the system sufficient to ensure it is functional and meets all applicable voting system standards.

4.4.1. Development. Test Plans shall be developed by an accredited laboratory. The plans shall utilize appropriate test protocols, standards or test suites developed by the laboratory. Laboratories must use all applicable protocols, standards or test suites issued by the EAC.

4.4.2. Required Testing. Test plans shall be developed to ensure that a voting system is functional and meets all requirements of the applicable voting system standards. The highest level of care and vigilance is required to ensure that comprehensive test plans are created. A test plan should ensure that the voting system meets all applicable standards and that test results and other factual evidence of the testing is clearly documented. System testing must meet the requirements of the VVSG. Generally, full testing will be required of any voting system applying for certification, regardless of prior certification history.

4.4.2.1. *New Systems*. New systems shall be subject to full testing of all hardware and software according to applicable voting system standards.

4.4.2.2. *Systems not previously EAC Certified*. Systems not previously certified by the EAC shall be fully tested as new systems.

4.4.2.3. *Modifications*. A modification to a previously EAC Certified voting systems shall be tested in manner to ensure all changes meet applicable voting system standards and that the modified system (as a whole) will properly and reliable function. The systems submitted for modification shall be subject to full

DRAFT

testing of the modifications and those systems or subsystems altered or impacted by the modification. The system will also be subject to system integration testing to ensure overall functionality. The modification will be tested to the version or versions of the VVSG presently accepted for testing and certification by the EAC. However, this does not mean that the full system must be tested to such standards. If the system has been previously certified to a VVSG version deemed acceptable by the EAC, it may retain that level of certification with only the modification being tested to the present version(s).

4.4.2.4. *Certification Upgrade*. Systems submitted for testing to new voting system standard (without modification) shall be tested in manner necessary to ensure that the systems meet all requirements of the new standards. Test Plans shall ensure that hardware and software components affected by changes in the standards are fully retested according to the new standards.

4.4.3. Format. Test labs shall issue test plans consistent with the requirements in the VVSG and any applicable EAC guidance.

4.4.4. EAC Approval. All test plans are subject to EAC approval. No test report will be accepted for technical review unless the test plan upon which it is based has been approved by EAC's Program Director.

4.4.4.1. *Review*. All test plans must be reviewed for adequacy by the Program Director. For each submission the Program Director will determine whether the test report is acceptable or unacceptable. Unacceptable plans will returned to the laboratory for further action. Acceptable plans will be approved. While manufacturers may direct test labs to begin testing before approval of a test plan, the manufacturer bears the full risk that the test plan (and thus any tests preformed) will be deemed unacceptable.

4.4.4.2. *Unaccepted Plans*. If a plan is not accepted, the Program Director will return the submission to the Manufacturer's identified laboratory for additional action. Notice of unacceptability will be provided in writing to the laboratory and include a description of the problems identified and steps required to remedy the test plan. Questions concerning the notice shall be forwarded to Program Director in writing. Plans that have not been accepted may be resubmitted for review after remedial action is taken.

4.4.4.3. *Effect of Approval*. Approval of a test plan is required before a test report may be filed. In most cases, approval of a test plan signifies that the tests proposed, if performed properly, are sufficient to fully test the system. However, a test plan is approved based upon the information submitted. New or additional information may require a change in testing requirements at any point in the certification process.

DRAFT

4.5. Testing. During testing, manufacturers are responsible for ensuring that VSTLs report any changes to a voting system or an approved test plan to the EAC. Manufacturers shall also ensure that VSTLs report all test failures or anomalies to the EAC.

4.5.1. Changes. Any changes to the voting system, initiated as a result of the testing process, will require submission of a new Technical Data Package and, potentially, an updated test plan. Any changes to or deviation from the test plan by a lab during the testing process will require resubmission of an updated test plan.

4.5.2. Test Anomalies or Failures. Manufacturers shall ensure that accredited laboratories notify the EAC of any test anomalies or failures during testing. This notice shall be in writing. Unless the laboratory can document (for EAC approval) that a failure was a result of testing methodology or execution, effected systems must be modified and the Technical Data Packages and Test Plans resubmitted.

4.6. Test Report. Manufactures shall have their identified test lab submit test reports directly to the EAC. Test reports shall be submitted only if the voting system has been successfully tested and all tests identified in the test report have been performed.

4.6.1. Submission. The test reports shall be submitted to the Program Director. The Program Director shall review the submission for completeness. Any reports showing incomplete or unsuccessful testing will be returned to the test laboratory for action and resubmission. Test reports shall be submitted in Adobe PDF, Microsoft Word or other electronic formats as prescribed by the Program Director. Information on how to submit reports will be posted on EAC's website.

4.6.2. Format. Manufacturers shall ensure that test labs submit reports consistent with the requirements in the VVSG.

4.6.3. Technical Review. A technical review of the test report, Technical Data Package and test plan will be conducted by technical experts. These EAC experts will submit a report outlining their findings to the Program Director. The report will provide an assessment of the completeness, appropriateness and adequacy of the VSTL's testing as documented in the test report

4.6.4. Program Director's Recommendation. The program director shall review the report. The Program Director shall either:

4.6.4.1. Recommend certification of the candidate system consistent with the reviewed test report and forward it to the Decision Authority for action (Initial Decision); or

4.6.4.2. Refer the matter back to the technical reviewers for additional specified action and resubmission.

DRAFT

4.7. Initial Decision on Certification. Upon receipt of the report and recommendation forwarded by the Program Director, the Decision Authority shall issue an Initial Decision on Certification. The decision shall be forwarded to the Manufacturer consistent with the requirements of this manual.

4.7.1. An Initial Decision granting certification shall be processed consistent with Chapter 5 of this manual.

4.7.2. An Initial Decision denying certification shall be processed consistent with Chapter 6 of this manual.

DRAFT

5. Grant of Certification

5.1. Overview. The grant of certification is the formal process through which EAC acknowledges that a voting system has successfully completed conformance testing to an appropriate set of standards or guidelines. The grant of certification begins with the initial decision of the Decision Authority. This decision becomes final after the manufacturer confirms that the final version of the software that was certified and which the manufacturer will deliver with the certified system has been subject to a trusted build, placed in an EAC approved repository and can be verified using the manufacturer's system identification tools. Once a certification is issued, the manufacturer is provided a Certificate of Conformance and relevant information about the system is added to the EAC website. Manufacturers with certified voting systems are responsible for ensuring that each system it produces is properly labeled as certified.

5.2. Applicability of this Chapter. This chapter applies when the Decision Authority makes an initial decision to grant a certification to a voting system based upon the materials and recommendation provided by the program director.

5.3. Initial Decision. The Decision Authority shall make and issue to a manufacturer a written decision on all voting systems submitted for certification. When such decisions result in a grant of certification, the decision shall be considered preliminary and referred to as an *Initial Decision* pending required action by the manufacturer. The Initial Decision shall:

5.3.1. State the preliminary determination reached (granting certification);

5.3.2. Inform the manufacturer of the steps that must be taken to make the determination final and receive a certification. This shall include providing the manufacturer with specific instructions, guidance and procedures for confirming that the final certified version of the software meets the requirements for:

5.3.2.1. Performing and documenting a trusted build pursuant to section 5.6 of this chapter, and

5.3.2.2. Depositing software in an approved repository pursuant to section 5.7 of this chapter.

5.3.2.3. Creating and making available system verification tools pursuant to section 5.8 of this chapter.

5.3.3. Certification is not final until the manufacturer accepts the certification and any and all conditions placed on the certification.

5.4. Pre-Certification Requirements. Before an initial decision becomes final and a certification is issued, manufacturers must ensure certain steps are taken. They must confirm that the final version of the software that was certified and which the manufacturer will deliver with the certified system has been subject to a trusted build (see section 5.6), deposited in an EAC approved repository (see section 5.7) and can be verified using manufacturer developed

DRAFT

identification tools (see section 5.8). The manufacturer must provide the EAC documentation demonstrating compliance with these requirements.

5.5. Trusted Build. A software build (also referred to as a compilation) is the process whereby source code is converted to machine readable binary instructions (executable code) for the computer. A "trusted build" (or trusted compilation) is a build performed with adequate security measures implemented to give confidence that the executable code is a verifiable and faithful representation of the source code. A trusted build creates a chain of evidence from the Technical Data Package and source code submitted for certification to the actual executable programs that are run on the system. Specifically, the build will:

5.5.1.1. Demonstrate that the software was built as described in the Technical Data Package;

5.5.1.2. Show that the tested and approved source code was actually used to build the executable code used on the system;

5.5.1.3. Demonstrate that no elements other than those included in the Technical Data Package were introduced in the software build; and

5.5.1.4. Document for future reference the configuration of the system certified.

5.6. Trusted Build Procedure. A trusted build is three step process: (1) the build environment is constructed, (2) the source code is loaded onto the build environment, and (3) the executable code is compiled and installation disk created. The process may be simplified for modification to previously certified systems. In each step, a minimum of two witnesses from different organizations are required to participate. These participants must include a VSTL representative and vendor representative. Prior to creating the trusted build the VSTL must complete the source code review of the software delivered from the vendor for compliance with the VVSG, and produce and record digital signatures of all source code modules. An instructive discussion of this process may be found in Appendix C.

5.6.1. Constructing the Build Environment. The VSTL shall construct the build environment in an isolated environment controlled by the VSTL, as follows:

5.6.1.1. The disk that will hold the build environment shall be completely erased by the VSTL to assure a total and complete cleaning of the disk. The VSTL shall use commercial off-the-shelf software (COTS), purchased by the laboratory, for cleaning the disk.

5.6.1.2. The VSTL, with vendor consultation and observation, shall construct the build environment.

5.6.1.3. After construction of the build environment, the VSTL shall produce and record a digital signature of the build environment.

DRAFT

5.6.2. Loading Source Code onto the Build Environment. After successful source code review, the VSTL shall load source code onto the build environment as follows:

5.6.2.1. The VSTL shall check the digital signatures of the source code modules and build environment to assure that they are unchanged from their original form.

5.6.2.2. The VSTL shall load the source code onto the build environment and produce and record the digital signature of the resulting combination.

5.6.2.3. The VSTL shall capture a disk image of the combination build environment and source code modules immediately prior to performing the build.

5.6.2.4. The VSTL shall deposit the disk image into an authorized archive to assure that the build can be reproduced if necessary, at a later date.

5.6.3. Creating the Executable Code. Upon completion of all the tasks outlined above, the VSTL shall produce the executable code.

5.6.3.1. The VSTL shall produce and record a digital signature of the executable code.

5.6.3.2. The VSTL shall deposit into an EAC approved software repository the executable code and create installation disk(s) from the executable code.

5.6.3.3. The VSTL shall produce and record digital signatures of the installation disk(s) in order to provide a mechanism to validate the software prior to installation on the voting system in a purchasing jurisdictions.

5.6.3.4. The VSTL shall install the executable code onto the system submitted for testing and certification prior to completion of system testing.

5.6.4. Trusted Build for Modifications. The process of building new executable code when a previously certified system has been modified is somewhat simplified.

5.6.4.1. The build environment used in the original certification is removed from storage and its digital signature verified.

5.6.4.2. After source code review the modified files are placed onto the verified build environment and new executable files are produced.

5.6.4.3. If the original build environment is unavailable or its digital signatures cannot be verified against those recorded from the original certification then the more labor intensive process of creating the build environment must be performed. Further source code review may be required of unmodified files to validate that they are unmodified from their originally certified versions.

DRAFT

5.7. **Depositing Software in an Approved Repository**. After EAC certification has been granted, the VSTL project manager, or an appropriate delegate of the project manager, shall deposit the following in one or more trusted archive(s) (repositories) designated by the EAC, such as the NIST NSRL.

5.7.1. Source code used for the trusted build and its digital signatures.

5.7.2. Disk image of the pre-build, build environment and any digital signatures to validate that it is unmodified.

5.7.3. Disk image of the post-build, build environment and any digital signatures to validate that it is unmodified.

5.7.4. Executable code produced by the trusted build and its digital signatures of all files produced.

5.7.5. Installation disk(s) and its digital signatures.

5.8. **System Identification Tools**. The manufacturer shall provide tools though which a fielded voting system may be identified and demonstrated to be unmodified from the system which was certified. The purpose of this requirement is to make such tools available to state, local and Federal officials to identify and verify that the equipment used in elections is unmodified from its certified version. Manufacturers may develop and provide these tools as they see fit. However, the tools must provide the means to identify and verify hardware and software. The EAC may review the system identification tools developed by the manufacture to ensure compliance. Examples of system identification methodology include:

5.8.1. Hardware is commonly identified by model and revision numbers on the unit, its printed wiring boards (PWB) and major subunits. Typically hardware is verified as unmodified by providing detailed photographs of the PWB's and internal construction of the unit. These may be used to compare to the unit being verified.

5.8.2. Software operating in on a host computer will typically be verified by providing a self-booting CD or similar device that verifies the digital signatures of the voting system application files AND the signatures of all non-volatile files that the application files access during their operation. Note that the creation of such a CD requires having a file map of all non-volatile files that are used by the voting system. Such a tool must be provided for verification using the digital signatures of the original executable files provided for testing. If during the certification process modifications are made and new executable files created then the tool must be updated to reflect the digital signatures of the final files to be distributed for use. For software operating on devices where a self-booting CD or similar device cannot be used a procedure must be provided to allow identification and verification of the software that is being used on the device.

5.9. **Documentation**. Manufacturers' shall provide documentation to the Program Director verifying that the trusted build has been performed, software has been deposited in an approved repository and that system identification tools are available to election officials. The Manufacturer shall submit a letter, signed by both its management representative and a VSTL

DRAFT

official, stating (under penalty of law) that it has (1) performed a trusted build consistent with the requirements of Section 5.6 of this Manual; (2) deposited software consistent with Section 5.7 of this Manual and (3) created and made available system identification tools consistent with Section 5.8 of this Manual. This letter shall also include (as attachments) a copy and description of the system identification tool developed under Section 5.8, above.

5.10. Agency Decision. Upon receipt of documentation demonstrating the successful completion of the requirements above and recommendation of the Program Director, the Decision Authority will issue an Agency Decision granting certification and providing the manufacturer with a certification number and Certificate of Conformance.

5.11. Certification Document. A Certificate of Conformance will be provided to manufacturers for voting systems which have successfully met the requirements of this program. The document will serve as the manufacturer's evidence that a particular system is certified to a particular set of voting system standards. The EAC certification and certificate applies only to the specific voting system configuration submitted and evaluated under the program. Any modification to the system not authorized by the EAC will void the certificate. The certificate will include the product (voting system) name, the specific model or version of the product tested, the name of the VSTL conducting the testing, identification of the standards to which the system was tested, the EAC Certification Number for the product, and the signature of the EAC Executive Director.

5.12. Certification Number and Version Control. Each system certified by the EAC will receive a certification number. This number is unique to the system and will remain with the system until such time as the system is decertified, sufficiently modified or tested and certified to newer standards. Generally, when a previously certified system is issued a new certification number, the manufacturer will be required to change the system's name or version number.

5.12.1. New voting systems and those not previously Certified by the EAC. All systems receiving their first certification from the EAC will receive a new Certification Number. Manufacturers must provide the EAC with the voting system's name and version number during the application process (Chapter 4). Systems previously certified by another body may retain the prior system name and version number unless the system was modified prior to its submission to the EAC. Such modified systems must be submitted with a new naming convention (i.e. new version number).

5.12.2. Modifications. Voting systems previously certified by the EAC and submitted for certification of a modification will generally receive a new voting system certification number. Such modified systems must be submitted with a new naming convention (i.e. new version number). In rare instances, the EAC may authorize retention of the same certification and naming convention when the modification is so minor that is does not represent a substantive change in the voting system. Request for such authorization must be made and approved by the EAC during application phase of the program.

5.12.3. Certification upgrade. Voting systems previously certified and submitted (without modification) for testing to a new version of the VVSG will receive a new certification

DRAFT

number. However, in such cases the manufacturer will not be required to change the systems name or version.

5.13. Publication of EAC Certification. The EAC will publish and maintain on its website a list of all certified voting systems including copies of all Certificates of Conformance, the supporting test report and information about the manufacturer. Note that ALL information contained in the test report and Technical Data Package EXCEPT that identified as confidential AT THE TIME OF SUBMISSION will be posted to the website. Such information will be posted immediately following the Manufacturer's receipt of the EAC Final Decision and Certificate of Conformance.

5.14. Representation of EAC Certification. Manufacturers may not represent or imply that a voting system is certified unless it has received a Certificate of Conformance for that system. Statements regarding EAC certification in brochures, websites, displays and advertising/sales literature must be made solely in reference to specific systems. Any action by a manufacturer to suggest EAC endorsement of their product or organization is strictly prohibited.

5.15. Mark of Certification Requirement. Manufacturers shall post a mark of certification on all EAC Certified voting systems produced. This mark or label must be permanently attached to the system prior to sale, lease or release to third parties. A mark of certification shall be made through the use of an EAC mandated template available for download on the EAC website. These templates identify the version of the VVSG or VSS to which the system is certified. Use of this template shall be mandatory. The EAC mark must be displayed as follows:

5.15.1. The Manufacturer may only use the mark of certification which accurately reflects the certification held by the system. In the event a system has components or modifications tested to various versions of the VVSG (or VSS) the system shall bear only one mark of certification. This shall be the mark of the oldest or least rigorous standard to which any component or modification of the system was tested.

5.15.2. The mark shall be placed on the outside of the voting system in a place readily available to election officials.

5.15.3. The notice shall be permanently affixed to the voting system. The label shall not be a paper label. "Permanently affixed" means that the label is etched, engraved, stamped, silk-screened, indelibly printed, or otherwise permanently marked on a permanently attached part of the equipment or on a nameplate of metal, plastic, or other material fastened to the equipment by welding, riveting, or a permanent adhesive.

5.15.4. The label must be designed to last the expected lifetime of the voting system in the environment in which the system may be operated and must not be readily detachable.

5.16. Information to Election officials purchasing voting systems. The user's manual or instruction manual for a certified voting system shall warn purchasers that changes or modifications not tested and certified by EAC will void the EAC certification of the voting system. In cases where the manual is provided only in a form other than paper, such as on a

DRAFT

computer disk or over the internet, the information required in this section may be included in this alternative format provided that the election official can reasonably be expected to have the capability to access information in that format.

DRAFT

DRAFT

6. Denial of Certification

6.1. Overview. When the Decision Authority issues an Initial Decision denying certification, the Manufacturer has certain rights and responsibilities. The Manufacturer may request an opportunity to cure the defects identified by the Decision Authority. Additionally, the Manufacturer may request the Decision Authority to reconsider the Initial Decision after the Manufacturer has had the opportunity to review the record and submit supporting written materials, data and rational for its position. Finally, in the event reconsideration is denied, the Manufacturer may appeal the decision to the Appeal Authority.

6.2. Applicability of this Chapter. This chapter applies when the Decision Authority makes an initial decision to deny an application for voting system certification based upon the materials and recommendation provided by the program director.

6.3. Form of Decisions. All agency determinations shall be made in writing. Moreover, all materials and recommendations reviewed or used by agency decision makers in arriving at an official determination shall be in written form.

6.4. Effect of Denial of Certification. Upon receipt of the agency's decision denying certification—or in the event of an appeal, the decision on appeal—the manufacturer's application for certification is finally denied. Such systems will not be reviewed again by the EAC for certification unless the manufacturer alters the system, retest it and submits a new application for system certification.

6.5. The Record. The Program Director shall maintain all documents related to a denial of certification. Such documents shall constitute the procedural and substantive record of the decision making process. Examples include:

6.5.1. The Program Director's report and recommendation to the Decision Authority;

6.5.2. The Decision Authority's Initial Decision and Final Decision;

6.5.3. Any materials gathered by the Decision Authority that served as a basis for a certification determination;

6.5.4. All relevant and allowable materials submitted by the Manufacturer upon request for reconsideration or appeal;

6.5.5. All correspondence between the EAC and a Manufacturer after the issuance of an Initial Decision denying certification.

6.6. Initial Decision. The Decision Authority shall make and issue a written decision on voting systems submitted for certification. When such decisions result in a denial of certification, the decision shall be considered preliminary and referred to as an *Initial Decision*. Initial Decisions shall be in writing and contain (1) the Decision Authority's basis and explanation for the decision and (2) notice of the manufacturer's rights in the denial of certification process:

6.6.1. Basis and Explanation. The Initial Decision of the Decision Authority shall:

6.6.1.1. Clearly state the agency's decision on Certification;

6.6.1.2. Explain the basis for the decision, including identifying:

6.6.1.2.1. the relevant facts,

6.6.1.2.2. the applicable EAC voting system standards (VVSG or VSS),

6.6.1.2.3. relevant analysis in the Program Director's recommendation, and

6.6.1.2.4. the reasoning behind the determination.

6.6.1.3. State the actions the manufacturer must take, if any, to cure all defects in the voting system and obtain a certification.

6.6.2. Manufacturer's Rights. The written Initial Decision must also inform the manufacture of its procedural rights under the program. These include:

6.6.2.1. Right to request reconsideration. The manufacturer shall be informed of its right to request a timely reconsideration. (see Section 6.9). Such request must be made within 20 days of the manufacturer's receipt of the Initial Decision.

6.6.2.2. Right to request a copy or otherwise have access to the information that served as the basis of the Initial Decision ("the record").

6.6.2.3. Right to cure system defects prior to final agency decision (see Section 6.8). A manufacturer may request an opportunity to cure within 20 days of its receipt of the Initial Decision.

6.7. No Manufacturer Action on Initial Decision. If a manufacturer takes no action (by either failing to request an opportunity to cure or request reconsideration) within 20 calendar days of its receipt of the initial decision, the initial decision shall become the agency's final decision on certification. In such cases, the manufacture is determined to have forgone its right to reconsideration, cure and appeal. The certification application shall be considered finally denied.

6.8. Opportunity to Cure. Within 20 calendar days of receiving the EAC's Initial Decision on certification, a manufacturer may request an opportunity to cure the defects identified in the EAC's Initial Decision. If the request is approved, a compliance plan must be created, approved and followed. If this cure process is successfully completed, a voting system denied certification in an Initial Decision may receive a certification without resubmission.

DRAFT

DRAFT

6.8.1. Manufacturer’s Request to Cure. The Manufacturer must send a request to cure within 20 calendar days of receipt of an initial decision. The request must be sent to the Program Director.

6.8.2. EAC Action on Request. The Decision Authority will review the request and approve it. The Decision Authority will deny a request to cure only if the proposed plan to cure is inadequate or does not present a viable way to remedy the identified defects. Approval or denial of a request to cure shall be provided the manufacturer in writing. If the manufacturer’s Request to Cure is denied, it shall have 20 days from the date it received such notice to request reconsideration of the Initial Decision pursuant to section 6.6.2.

6.8.3. Manufacturer’s Compliance Plan. Upon approval of the manufacturer’s request for an opportunity to cure, it shall submit a compliance plan to the Decision Authority for approval. This compliance plan must set forth steps to be taken to cure all identified defects. It shall include the proposed changes to the system, an updated technical data package, a test plan (limited to those tests required by the proposed changes), and provide for the testing of the amended system and submission of the test report to the EAC for approval. It should also provide an estimated date for receipt of the test report and include a schedule of periodic progress reports to the Program Director.

6.8.4. EAC Action on the Compliance Plan. The Decision Authority must review and approve the compliance plan. The Decision Authority may require the manufacturer to provide additional information and modify the plan as required. If the Manufacturer is unable or unwilling to provide a compliance plan acceptable to the Decision Authority, the Decision Authority shall provide written notice terminating the “opportunity to cure” process. The Manufacturer shall have 20 calendar days from the date it received such notice to request reconsideration of the Initial Decision pursuant to section 6.6.2.

6.8.5. Manufacturer’s Issuance of the Compliance Plan Test Report. The manufacturer shall submit the test report created pursuant to its EAC-approved compliance plan. The EAC shall review the test report, along with the original test report and other materials originally provided. The report will be technically reviewed by the EAC consistent with the procedures laid out in Chapter 4 of this Manual.

6.8.6. EAC Decision on the System. After receipt of the test plan, the Decision Authority shall issue a decision on a voting system amended pursuant to an approved compliance plan. This decision shall be issued in the same manner and with the same process and rights as an initial decision on certification.

6.9. Requests for Reconsideration. Manufacturers may request reconsideration of an Initial Decision.

6.9.1. Submission of Request. A request for reconsideration must be made within 20 days of the Manufacturer’s receipt of an Initial Decision. The request shall be made and sent to the Decision Authority.

6.9.2. Acknowledgement of Request. The Decision Authority shall acknowledge receipt of the manufacturer's request for reconsideration. This acknowledgement shall either enclose all information that served as the basis for the Initial Decision (the record) or provide a date by which the record will be forwarded to the manufacturer.

6.9.3. Manufacturer Submissions. Within 30 days of receipt of the record, a manufacturer may submit written materials in support of its position. This includes:

6.9.3.1. A written argument responding to the conclusions in the Initial Decision.

6.9.3.2. Documentary evidence relevant to the issues raised in the Initial Decision.

6.9.3.3. Other written materials created to provide relevant facts (such as additional test data, technical analyses and statements).

6.9.4. Decision Authority's Review of Request. The Decision Authority shall review and consider all relevant submissions of the manufacturer. In making a decision on reconsideration, the Decision Authority shall also consider all documents that make up the record and any other documentary information he or she determines relevant.

6.10. Agency Final Decision. The Decision Authority shall issue a written Agency Decision after review of the manufacturer's request for reconsideration. This Decision shall be the decision of the agency. The decision shall:

6.10.1.1. Clearly state the agency's determination on the application for certification;

6.10.1.2. Address the issues raised by the manufacturer in its request for reconsideration;

6.10.1.3. Identify all facts, evidence and EAC voting system standards (VVSG or VSS), that served as the basis for the decision;

6.10.1.4. Provide the reasoning behind the determination;

6.10.1.5. Identify and provide, as an attachment, any additional documentary information that served as a basis for the decision and that was not part of the manufacturer's submission or the prior record; and

6.10.1.6. Provide the manufacturer notice of its right to appeal.

6.11. Appeal of Agency Final Decision. A manufacturer may, upon receipt of an Agency Final Decision denying certification, issue a request for appeal.

6.11.1. Requesting Appeal.

DRAFT

6.11.1.1. *Submission*. Requests must be submitted in writing to the Program Director, addressed to Chair of the U.S. Election Assistance Commission.

6.11.1.2. *Timing of Appeal*. The manufacturer may request an appeal within 20 calendar days of receipt of the Agency Final Decision. Late requests will not be considered.

6.11.1.3. *Contents of Request*.

6.11.1.3.1. The request must clearly state the specific conclusions of the Final Decision it wishes to appeal.

6.11.1.3.2. The request may include additional written argument.

6.11.1.3.3. The request may not reference or include any factual material not in the record.

6.11.2. <u>Consideration of Appeal</u>. All timely appeals will be considered by the appeal authority.

6.11.2.1. The appeal authority shall be two or more U.S. EAC Commissioners or other individual or individuals appointed by the Commissioners who have not previously served as the initial or reconsideration authority on the matter.

6.11.2.2. All decisions on appeal shall be based on the record.

6.11.2.3. The decision of the Decision Authority shall be given deference by the appeal authority. While it is unlikely that the scientific certification process will produce factual disputes, in such cases, the burden of proof shall belong to the Manufacturer to demonstrate by clear and convincing evidence that their voting system met all substantive and procedural requirements for certification. In other words, the determination of the Decision Authority will be overturned only when the appeal authority finds the ultimate facts in controversy highly probable.

6.12. Decision on Appeal. The appeal authority shall make a written, final Decision on Appeal. This Decision on Appeal shall be provided the Manufacturer.

6.12.1. <u>Contents</u>. The Decision on Appeal shall:

6.12.1.1. State the final determination of the agency;

6.12.1.2. Address the matters raised by the Manufacturer on appeal;

6.12.1.3. Provide the reasoning behind the decisions; and

6.12.1.4. State that the decision on appeal is final.

DRAFT

6.12.2. Determinations. The appeal authority may make one of three determinations.

6.12.2.1. *Approval of Certification.* The Appeal Authority may overturn the decision of the Decision Authority and grant the appeal in full. In such cases, certification will be approved subject to the requirements of Chapter 5.

6.12.2.2. *Denial of Certification.* The Appeal Authority may uphold the decision of the Decision Authority and deny the appeal in full. In such cases the application for appeal is finally denied.

6.12.2.3. *Grant of Appeal in Part with Opportunity to Cure.* The Appeal Authority may grant the appeal in part. This will only occur in instances where the denied issues on appeal may be cured. In such cases, the Manufacturer must cure the identified discrepancies prior to the grant of certification. The appeal authority shall remand the matter to the Decision Authority to initiate to cure process consistent with the decision.

6.12.2.3.1. If the Manufacturer successfully completes the cure process, the certification will be approved by the Decision Authority subject to the requirements in Chapter 5.

6.12.2.3.2. If the Decision Authority determines the cure process to have failed, he or she shall submit a report to the Appeal Authority (with a copy to the Manufacturer) for final determination. If the Appeal Authority concurs with the report, the Appeal Authority shall issue a Second Decision on Appeal denying certification. If the Appeal Authority disagrees with the Decision Authority, the matter shall be remanded back to the Decision Authority with specific instructions.

6.12.3. Effect. All Decisions on Appeal shall be final and binding on the Manufacturer. No additional appeal shall be granted.

DRAFT

DRAFT

7. Decertification

7.1. Overview. Decertification is the process by which the EAC revokes a Certification previously granted to a voting system. It is an important part of the Certification Program, as it serves to ensure that the requirements of the program are followed and that certified voting systems fielded for use in our Federal elections maintain the same level of quality as those presented for testing. Decertification, is a serious matter. Its use will have a significant impact on Manufacturers, State and local governments, the public and the administration of elections. As such, the process for decertification is involved. It is initiated when the EAC receives information that a voting system may not be in compliance with the Voluntary Voting System Guidelines or the procedural requirements of this manual. Upon receipt of such information, the Program Director may initiate an Informal Inquiry to determine the credibility of the information. If the information is credible and suggests the system is noncompliant, a Formal Investigation will be initiated. If the results of the Formal Investigation demonstrate noncompliance, the manufacturer will be provided a Notice of Non-Compliance. Before a final decision on decertification is made, the manufacturer will have the opportunity to remedy any defects identified in the voting system and present information for consideration by the decertification authority. A decertification of a voting system may be timely appealed.

7.2. Decertification Policy. Voting systems certified by the EAC are subject to Decertification. Systems shall be decertified if they (1) are shown not to meet applicable Voluntary Voting System Guideline Standards, (2) have been modified without following the requirements of this manual or (3) the Manufacturer has otherwise failed to follow the procedures outlined in this manual such that the quality, configuration or compliance of the system is in question. Decertification of a voting system is a serious matter. Systems will be decertified only after completion of the process outlined in this chapter.

7.3. Informal inquiry. An Informal Inquiry is the first step taken when information is presented to the EAC that suggests a voting system may not be in compliance with the Voluntary Voting System Standards or the procedural requirements of this Manual.

7.3.1. Informal Inquiry Authority. The authority to conduct an Informal Inquiry shall rest with the Program Director.

7.3.2. Purpose. The purpose of the informal inquiry is solely to determine whether a formal investigation is warranted. The outcome of an informal inquiry is limited to a decision on referral for investigation.

7.3.3. Procedure. Informal Inquiries do not follow a formal process.

7.3.3.1. *Initiation*. Informal Inquiries are initiated at the discretion of the Program Director. They may be initiated any time the Program Director receives attributable, relevant information that suggests a certified voting system may require decertification. The information shall come from a source which has directly observed or witnessed the reported occurrence. Such information may be a product of the Certification Quality Monitoring Program (see

Chapter 8). Information may also come from state and local election officials or voters who have used a given voting system. The Program Director may notify a Manufacturer that an Informal Inquiry has been initiated, but this is not required. Initiation of an inquiry shall be documented through the creation of a memorandum for the record.

7.3.3.2. *Inquiry*. The informal inquiry process is limited to that inquiry necessary to determine whether a Formal Investigation is required. In other words, the Program Director shall conduct such inquiry necessary to determine (1) that the information obtained is credible and (2) that the information, if true, would serve as a basis for decertification. There is no set procedure for an inquiry. The nature and extent of the inquiry process will vary depending upon the source of the information. For example, an informal inquiry initiated as a result of action taken under the Quality Monitoring Program will often require the Program Director merely to read the report issued as a result of the Quality Monitoring action. On the other hand, information provided by voters who have used a voting system or election officials may require the Program Director (or assigned technical experts) to perform an in-person inspection or make inquiries of the manufacturer.

7.3.3.3. *Conclusion*. An inquiry shall be concluded once the Program Director is in a position to determine the credibility of the information which initiated the inquiry and whether that information, if true, would require decertification. The Program Director may make only two conclusions: (1) Refer the matter for a formal investigation or (2) Close the matter without additional action.

7.3.4. Closing the Matter without Referral. If the Program Director determines, after informal inquiry, that a matter does not require a Formal Investigation, the Program Director shall close the inquiry by filing a Memorandum for Record. This document shall state the findings of the inquiry and the reasons a Formal Investigation was not warranted.

7.3.5. Referral. If the Program Director determines, after informal inquiry, that a matter requires a Formal Investigation, the Program Director shall refer the matter in writing to the Decision Authority. This referral shall:

7.3.5.1. State the facts that served as the basis for the referral.

7.3.5.2. State the findings of the Program Director.

7.3.5.3. Attach all documentary evidence that served as the basis for the conclusion.

7.3.5.4. Recommend a formal investigation, specifically stating the system to be investigated and the scope and focus of the proposed investigation.

DRAFT

DRAFT

7.4. Formal Investigation. A Formal Investigation is an official investigation to determine whether a voting system requires decertification. The end result of a Formal Investigation is a Report of Investigation.

7.4.1. Formal Investigation Authority. The Decision Authority shall have the authority to initiate and conclude a Formal Investigation by the EAC.

7.4.2. Purpose. The purpose of a Formal Investigation is to gather and document relevant information sufficient to make a determination on whether an EAC certified voting system requires decertification consistent with the policy put forth in Section 7.2, above.

7.4.3. Initiation of Investigation. The Decision Authority shall authorize the initiation of an EAC Formal Investigation.

7.4.3.1. *Scope*. The Decision Authority shall clearly set the scope of the investigation by identifying (in writing) the voting system (or systems) and specific procedural or operational non-conformance to be investigated. The non-conformance or non-conformances to be investigated shall be set forth in the form of numbered allegations.

7.4.3.2. *Investigator*. The Program Director shall be responsible for conducting the investigation unless another individual is appointed by the Decision Authority. The Program Director (or Decision Authority appointee) may assign staff or technical experts as required to investigate the matter.

7.4.4. Notice of Formal Investigation. Upon initiation of a Formal Investigation, notice shall be given the Manufacturer of the scope of the investigation. This notice shall:

7.4.4.1. Identify the voting system and specific procedural or operation non-conformance being investigated (scope of investigation).

7.4.4.2. Provide the Manufacturer an opportunity to provide relevant information in writing.

7.4.4.3. Provide an estimated timeline for the investigation.

7.4.5. Investigation. Due to the vital role voting systems play in our democratic process, investigations shall be conducted impartially, diligently, promptly and confidentially. Investigators shall use techniques to gather necessary information that meet these requirements.

7.4.5.1. *Fair and Impartial Investigation*. All Formal Investigations shall be conducted in a fair and impartial manner. All individuals assigned to an investigation must be free from any financial conflict of interest.

7.4.5.2. *Diligent Collection of Information*. All investigations shall be conducted in a meticulous and thorough manner. Investigations shall gather all relevant information and documentation that is reasonably available. The diligent collection of information is vital for informed decision making.

7.4.5.3. *Prompt Collection of Information*. Determinations which may affect the administration of Federal Elections must be made with all reasonable speed. EAC determinations on decertification will impact the actions of state and local election officials conducting elections. As such, all investigations regarding decertification must proceed with an appropriate sense of urgency.

7.4.5.4. *Confidential Collection of Information*. Consistent with Federal Law, information pertaining to a Formal Investigation should not be made public until the Report of Investigation is complete. The release of incomplete and unsubstantiated information or pre-decisional opinions which may be contrary or inconsistent with the final determination of the EAC, could cause public confusion or unnecessarily negatively effect public confidence in active voting systems. Such actions could serve to impermissibly impact election administration and voter turnout. All pre-decisional investigative materials must be appropriately safeguarded.

7.4.5.5. *Methodologies*. Investigators shall gather information by means consistent with the four principals noted above. Investigative tools include (but are not limited to):

7.4.5.5.1. Interviews. Investigators may interview individuals with relevant information (such as state and local election officials, voters with relevant information or representatives of the Manufacturer). All interviews shall be reduced to written form, the interview should be summarized in a statement that is reviewed, approved and signed by the subject.

7.4.5.5.2. Field Audits.

7.4.5.5.3. Manufacturer Site Audits.

7.4.5.5.4. Written Interrogatories. Investigators may pose specific, written questions to the manufacturers for the purpose of gathering information relevant to the investigation. The manufacturer shall respond to the queries within a reasonable timeframe (as specified in the request).

7.4.5.5.5. System Testing. Testing may be performed in an attempt to reproduce a condition or failure that has been reported.

DRAFT

7.4.5.6. *Report of Investigation*. The end result of a Formal Investigation is a Report of Investigation.

7.4.6. Report of Investigation. The Report of Investigation serves, primarily, to document (1) all relevant and reliable information gathered in the course of the investigation and (2) the conclusion reached by the Decision Authority.

7.4.6.1. *When Complete*. The report is complete and final when certified and signed by the Decision Authority.

7.4.6.2. *Contents of Report*. The written report shall:

7.4.6.2.1. Restate the scope of the investigation, identifying the voting system and specific matter investigated;

7.4.6.2.2. Briefly describe the investigative process employed;

7.4.6.2.3. Summarize the relevant and reliable facts and information gathered in the course of investigation;

7.4.6.2.4. Attach all relevant and reliable evidence collected in the course of investigation that documents the facts. All fact shall be documented in written form;

7.4.6.2.5. Analyze the information gathered; and

7.4.6.2.6. Clearly state the findings of the investigation.

7.4.7. Findings, Report of Investigation. The Report of Investigation shall state one of two conclusions. After gathering and reviewing all applicable facts the report shall find each allegation investigated to be either (1) substantiated or (2) unsubstantiated.

7.4.7.1. *Substantiated Allegations*. An allegation is substantiated if a preponderance of the relevant and reliable information gathered requires that the voting system at issue be decertified (consistent with the policy set out in Section 7.2). If any allegation is substantiated a Notice of Non-Compliance must be issued.

7.4.7.2. *Unsubstantiated Allegations*. An allegation is unsubstantial if the preponderance of the relevant and reliable information gathered does not require decertification (see Section 7.2). If all allegations are unsubstantiated, the matter shall be closed and a copy of the report forwarded to the Manufacturer.

7.4.8. Publication of Report. The report shall not be made public nor released to the public until final.

DRAFT

7.5. Effect of Informal Inquiry or Formal Investigation on Certification. A voting system's EAC Certification is not affected by the initiation or conclusion of an Informal Inquiry or Formal Investigation. Systems under investigation remain certified until a final Decision on Decertification is issued by the EAC.

7.6. Notice of Non-Compliance. If an allegation in a Formal Investigation is substantiated, the Decision Authority shall send the Manufacturer a Notice of Non-Compliance. The Notice of Non-Compliance is not, itself, a decertification of the voting system. The purpose of the notice is (1) to notify the Manufacturer of the non-compliance and (2) inform the Manufacturer of its procedural rights so that it may be heard prior to decertification.

7.6.1. Noncompliance Information. The Notice of Non-Compliance shall:

7.6.1.1. Provide Manufacturer a copy of the Report of Investigation;

7.6.1.2. Identify the noncompliance, consistent with the Report of investigation;

7.6.1.3. Inform Manufacturer that if the voting system is not made compliant, the voting system will be decertified.

7.6.1.4. State the actions the manufacturer must take, if any, to bring the voting system into compliance and avoid decertification.

7.6.2. Manufacturer's Rights. The written Initial Decision must also inform the manufacturer of its procedural rights under the program. These include:

7.6.2.1. *Right to Present Information Prior to Decertification Decision*. The manufacturer shall be informed of its right to present information to the Decision Authority prior to a determination of decertification.

7.6.2.2. *Right to have access to the information that will serve as the basis of the Decertification Decision*. The manufacturer shall be provided the Report of Investigation and any other materials that will serve as the basis of an agency Decision on Decertification.

7.6.2.3. *Right to cure system defects prior to Decertification Decision*. A manufacturer may request an opportunity to cure within 20 days of its receipt of the Notice of Non-Compliance.

7.7. Procedure for Decision on Decertification. The Decision Authority shall make and issue a written Decision on Decertification whenever a Notice of Non-Compliance is issued. The Decision Authority will not take such action until the Manufacturer has had a reasonable opportunity to cure the non-compliance and submit information for consideration.

7.7.1. Opportunity to Cure. The Manufacturer shall have an opportunity to *timely* cure a non-conformant voting system prior to decertification. Cure is timely when the cure process

DRAFT

can be completed prior to the next Federal Election. This means that any proposed cure must be in place before *any* individual jurisdiction fielding the system holds a Federal election. The Manufacturer must request the opportunity to cure. If the request is approved, a compliance plan must be created, approved and followed. If this cure process is successfully completed, a Manufacturer may modify a non-compliant voting system, remedy procedural discrepancies or otherwise bring its system into compliance without resubmission or decertification.

7.7.1.1. *Manufacturer's Request to Cure*. Within 20 calendar days of receiving the EAC's Notice of Non-Compliance, a manufacturer may request an opportunity to *timely* cure all defects identified in the Notice of Non-Compliance. The request must be sent to the Decision Authority and outline how the Manufacturer would modify the system, update the technical data package, create a test plan, test the system and obtain EAC approval prior to the next election for Federal office.

7.7.1.2. *EAC Action on Request*. The Decision Authority will review the request and approve it if the defects identified in the Notice of Non-Compliance may reasonably be cured prior to the next election for Federal office.

7.7.1.3. *Manufacturer's Compliance Plan*. Upon approval of the manufacturer's request for an opportunity to cure, the manufacturer shall submit a compliance plan to the Decision Authority for approval. This compliance plan must put forth the steps to be taken (including time frames) to cure all identified defects in a timely manner. The plan shall describe the proposed changes to the system, provide for modification of the system, update the technical data package, create a test plan (limited to those tests required by the proposed changes), and provide for the testing of the system and submission of the test report to the EAC for approval. The plan shall also include a schedule of periodic progress reports to the Program Director.

7.7.1.4. *EAC Action on the Compliance Plan*. The Decision Authority must review and approve the compliance plan. The Decision Authority may require the manufacturer to provide additional information and modify the plan as required. If the Manufacturer is unable or unwilling to provide a Compliance Plan acceptable to the Decision Authority, the Decision Authority shall provide written notice terminating the "opportunity to cure" process.

7.7.1.5. *Manufacturer's Submission of the Compliance Plan Test Report*. The manufacturer shall submit the test report created pursuant to its EAC approved Compliance Plan. The EAC shall review the test report and any other necessary or relevant materials. The report will be technically reviewed by the EAC in a manner similar to the procedures laid out in Chapter 4 of this Manual.

DRAFT

7.7.1.6. *EAC Decision on the System*. After receipt of the test plan, the Decision Authority shall issue a decision on a voting system amended pursuant to an approved Compliance Plan. For the purposes of planning, manufacturers should allow <u>at least</u> 20 working days for this process.

7.7.2. <u>Opportunity to be Heard</u>. The Manufacturer may submit written materials in response to the Notice of Non-Compliance and Report of Investigation. These documents shall be considered by the Decision Authority when making a determination on decertification. The Manufacturer shall ordinarily have 20 calendar days from the date it received the Notice of Non-Compliance (or in the case of a failed effort to cure, the termination of that process) to deliver its submissions to the Decision Authority. However, when warranted by the public interest (because a delay in making a determination on decertification would effect the timely, fair and effective administration of Federal elections), the Decision Authority may provide a Manufacturer less time to submit information. This alternative period (and the basis for it) must be stated in the Notice of Non-Compliance. The alternative time period must allow the manufacturer a reasonable amount of time to gather its submissions. Submissions may include:

7.7.2.1. A written argument responding to the conclusions in the Notice of Non-Compliance or Report of Investigation.

7.7.2.2. Documentary evidence relevant to the allegations or conclusions in the Notice of Non-Compliance.

7.7.2.3. Other written materials created to provide relevant facts (such as technical information, testing data or statements).

7.7.3. <u>Decision on Decertification</u>. The Decision Authority shall make an agency determination on Decertification.

7.7.3.1. *Timing*. The Decision Authority shall promptly make a decision on Decertification. However, the Decision Authority may not issue such a decision until the Manufacturer has provided all of its written materials for consideration or the time allotted for submission (usually 20 calendar days) has run.

7.7.3.2. *Considered Materials*. The Decision Authority shall review and consider all relevant submissions of the manufacturer. In make a decision on decertification, the Decision Authority shall also consider all documents that make up the record and any other documentary information he or she determines relevant.

7.7.3.3. *Agency Decision*. The Decision Authority shall issue a written Agency Decision after review of applicable materials. This decision shall be the final decision of the agency. The decision shall:

DRAFT

7.7.3.3.1. Clearly state the agency's determination on the decertification, specifically addressing the areas of non-compliance investigated;

7.7.3.3.2. Address the issues raised by the manufacturer in the materials it submitted for consideration;

7.7.3.3.3. Identify all facts, evidence, procedural requirements and/or voting system standards (VVSG or VSS) that served as the basis for the decision;

7.7.3.3.4. Provide the reasoning behind the determination;

7.7.3.3.5. Identify and provide, as an attachment, any additional documentary information that served as a basis for the decision and that was not part of the manufacturer's submission or the Report of Investigation; and

7.7.3.3.6. Provide the manufacturer notice of its right to appeal.

7.8. Effect of Decision Authority's Decision on Decertification. The Decision Authority's Decision on Decertification is the decision of the agency. A decertification is effective upon the manufacturer's receipt of the decision. A manufacturer that has had a voting system decertified may appeal that decision.

7.9. Appeal of Decertification. A manufacturer may, upon receipt of an Agency Final Decision on Decertification, timely request an appeal.

7.9.1. Requesting Appeal.

7.9.1.1. *Submission*. Requests must be submitted in writing to the Chair of the U.S. Election Assistance Commission.

7.9.1.2. *Timing of Appeal*. The manufacturer may request an appeal within 20 days of receipt of the Agency Final Decision on Decertification. Late requests will not be considered.

7.9.1.3. *Contents of Request*.

7.9.1.3.1. The request must clearly state the specific conclusions of the Final Decision it wishes to appeal.

7.9.1.3.2. The request may include additional written argument.

7.9.1.3.3. The request may not reference or include any factual material not previously considered or submitted to the EAC.

DRAFT

7.9.1.4. *Effect of Appeal on Decertification*. The initiation of an appeal does not impact the decertified status of a voting system. Systems are decertified upon notice of decertification in the agency's Decision on Decertification (see Section 7.8).

7.9.2. Consideration of Appeal. All timely appeals will be considered by the appeal authority.

7.9.2.1. The appeal authority shall be two or more U.S. EAC Commissioners or other individual or individuals appointed by the Commissioners who have not previously served as investigators, advisors or decision makers in the decertification process.

7.9.2.2. All decisions on appeal shall be based on the record.

7.9.2.3. The decision of the Decision Authority shall be given deference by the appeal authority. While it is unlikely that the scientific certification process will produce factual disputes, in such cases, the burden of proof shall belong to the Manufacturer to demonstrate by clear and convincing evidence that their voting system met all substantive and procedural requirements for certification. In other words, the determination of the Decision Authority will be overturned only when the appeal authority finds the ultimate facts in controversy highly probable.

7.9.3. Decision on Appeal. The appeal authority shall make a written, final Decision on Appeal. This decision shall be provided the Manufacturer. All Decisions on Appeal shall be final and binding on the Manufacturer. No additional appeal shall be granted. The Decision on Appeal shall:

7.9.3.1. State the final determination of the agency;

7.9.3.2. Address the matters raised by the Manufacturer on appeal;

7.9.3.3. Provide the reasoning behind the decisions; and

7.9.3.4. State that the decision on appeal is final.

7.9.4. Effect of Appeal.

7.9.4.1. *Grant of Appeal*. If a manufacturer's appeal is granted in whole, the decision of the Decision Authority is reversed. The voting system shall have its certification reinstated. For the purposes of this program, the system shall be treated as though it was never decertified.

DRAFT

7.9.4.2. *Denial of Appeal*. If a manufacturer's appeal is denied (in whole or in part), the decision of the Decision Authority is upheld. The voting system remains decertified and no additional appeal is available.

7.10. Effect of Decertification. Voting systems that have been decertified no longer hold an EAC Certification under the program. For the purposes of this manual and the program, such systems will be treated as any other uncertified voting system. As such:

7.10.1. The manufacturer may not represent the voting system as certified;

7.10.2. The voting system may not be labeled as certified;

7.10.3. The voting system will be removed from the EAC list of Certified Systems; and

7.10.4. The EAC will notify state and local election officials of the decertification.

7.11. Recertification. A decertified system may be re-submitted for certification. Such systems shall be treated as any other system seeking certification. The Manufacturer shall present an application for certification consistent with this manual.

DRAFT

8. Quality Monitoring Program

8.1. Overview. The quality of any product, including a voting system, depends on two specific elements: (1) the design of the product or system; and (2) the care and consistency of the manufacturing process. The EAC testing and certification process focuses on voting system design by ensuring that a representative sample of a system meets the technical specifications of the applicable EAC voting system standards. This is process is commonly called 'type acceptance'. It determines whether the representative sample submitted for testing meets the requirements. What type acceptance does not do is explore whether variations in manufacturing may allow production of non-compliant systems. Generally, the quality of the manufacturing is the responsibility of the manufacturer. Once a system is certified, the vendor assumes primary responsibility for compliance of the produced products. This is accomplished by the manufacturer's configuration management and quality control processes. However, the EAC's Quality Monitoring Program, as outlined in this chapter, provides an additional layer of quality control by allowing the EAC to perform manufacturing site reviews, carry out fielded system reviews and gather information on voting system anomalies from election officials. These are additional tools to help assure that voting systems continue to meet the requirements of EAC's voting system standards as they are manufactured, delivered and used in elections. These aspects of the program allow the EAC to independently monitor the continued compliance of fielded voting systems.

8.2. Purpose. The purpose of the Quality Monitoring Program is to ensure that the voting systems certified by the EAC are identical to those fielded in election jurisdictions. This is done primarily by identifying: (1) potential quality problems in manufacturing, (2) uncertified voting system configurations and (3) field performance issues with certified systems.

8.3. Manufacturer Quality Control. EAC's Quality Monitoring Program is not a substitute for the manufacturer's quality control program. As stated in Chapter 2 of this manual, all manufacturers must have an acceptable quality control program in place before they may be registered. The EAC's program serves as an independent and complimentary process of quality control which works in tandem with manufacturer's efforts.

8.4. Quality Monitoring Methodology. This chapter provides the EAC with three primary tools it will use to assess the level of effectiveness of the certification process and the compliance of fielded voting systems. These tools include (1) manufacturing site reviews, (2) fielded system reviews and (3) a means to receive anomaly reports from the field.

8.5. Manufacturing Site Review. Facilities that produce certified voting systems will be reviewed periodically, at the discretion of the EAC, to verify that the system being manufactured, shipped and sold is the same as the sample submitted for certification testing. All registered manufacturers must cooperation with such audits as a condition of program participation.

8.5.1. Notice. The site review may be scheduled or unscheduled, at the discretion of the EAC. Unscheduled reviews will be performed with at least 24 hours notice. Scheduling and notice of site reviews will be coordinated with and provided to both the manufacturing facility representative and the Manufacturer's representative.

DRAFT

8.5.2. Frequency. At a minimum, one or more manufacturing facilities of a registered manufacturer shall be subject to a site review at least once every four years.

8.5.3. The Review. The production facility and production test records must be made available for review. When requested, production schedules must be provided to the EAC. Production or production testing may be witnessed by EAC representatives. If equipment is not being produced during the inspection, the review may be limited to production records. During the inspection, the manufacturer must make available to the EAC representative the manufacturer's quality manual and other documentation sufficient to enable the inspector to evaluate the facility's:

8.5.3.1. Manufacturing quality controls;

8.5.3.2. Final inspection and testing;

8.5.3.3. History of deficiencies or anomalies and corrective actions taken;

8.5.3.4. Equipment calibration and maintenance;

8.5.3.5. Corrective action program;

8.5.3.6. Policies on product labeling and the application of the EAC mark of certification; and

8.5.4. Exit Briefing. Site reviewers will provide the manufacturing facility representative a verbal exit briefing regarding the preliminary observations of the review.

8.5.5. Written Report. A written report documenting the review will be drafted by the EAC representative and provided to the manufacturer. The report will detail the findings of the review and identify actions that are required to correct any deficiencies.

8.6. Fielded System Review and Testing. Upon invitation or with the permission of a state or local election authority, the EAC may, at its discretion, conduct a review of fielded voting systems. Such reviews will be done to ensure that a fielded system is in the same configuration as that certified by the EAC and that it has the proper mark of certification. This review may include the testing of a fielded system, if deemed necessary. Any anomalies found during this review and testing will be provided to the election jurisdiction and the manufacturer.

8.7. Field Anomaly Reporting. The EAC will collect information from election officials who field EAC certified voting systems as another means of gathering field data. Information on actual voting system field performance is a basic means to assess the effectiveness of certification program and the manufacturing quality and version control. The EAC will provide a mechanism for election officials to provide real world input on voting system anomalies.

DRAFT

8.7.1. Anomaly Report. An anomaly report is a form that election officials may use to report voting system anomalies to the EAC. The form (and instructions for its completion) are available at Appendix D or on the EAC website, www.eac.gov. The form may be filed with the EAC on-line or by mail. Use of the form is required.

8.7.2. Who May Report? Reports may be filed by state or local election officials who have experienced voting system anomalies in their jurisdiction. The individuals reporting must identify themselves and have firsthand knowledge or official responsibility over the anomaly being reported. Anonymous or hearsay reporting will not be accepted.

8.7.3. What Is Reported? Election officials shall report voting system anomalies. An "anomaly" is defined as an irregular or inconsistent action or response from the voting system or system component resulting in some disruption to the election process. Incidents resulting from administrator error or procedural deficiencies are not considered an anomaly for the purposes of this chapter. Officials must report:

8.7.3.1. Their name, title, contact information and jurisdiction;

8.7.3.2. A description of the voting system at issue;

8.7.3.3. The date and location of the reported occurrence;

8.7.3.4. The type of election; and

8.7.3.5. A description of the anomaly witnessed.

8.7.4. Report Distribution. Credible reports will be distributed to state and local election jurisdictions who field similar systems and the manufacturer of the voting system at issue.

8.8. Use of Quality Monitoring Information. Ultimately, the information the EAC gathers from manufacturing site reviews, fielded system reviews and field anomaly reports will be used to improve the program and ensure the quality of voting systems. The system is not designed to be punitive, but focused on improvement of the process. Information gathered will be used to:

8.8.1. Identify areas for improvement in the EAC's testing and certification program;

8.8.2. Improve manufacturing quality and change control processes;

8.8.3. increase voter confidence in voting technology;

8.8.4. Inform manufacturers, election officials and the EAC of issues associated with voting systems in a real world environment;

8.8.5. Share information between jurisdictions who utilize similar voting systems;

DRAFT

8.8.6. Resolve problems associated with voting technology or manufacturing in a timely fashion by involving manufacturers, election officials and the EAC;

8.8.7. Provide feedback to the EAC, NIST and the TDGC regarding issues which may need to be addressed through a revision to the Voluntary Voting System Guidelines;

8.8.8. Initiate an investigation where information suggests that decertification is warranted (See Chapter 7).

DRAFT

9. Interpretations

9.1. Overview. A request for Interpretation is a means by which a registered manufacturer or VSTL may seek clarification on a specific EAC voting system standard (VVSG or VSS). Interpretations are clarifications of the voting system standards and guidance on how to properly evaluate conformance to it. Suggestions or requests for modifications to the standards are provided by other processes. This chapter outlines the policy, requirements and procedure for requesting an Interpretation.

9.2. Policy. Registered Manufacturers or VSTLs may request that the EAC provide a definitive interpretation of EAC accepted voting system standards (VVSG or VSS) when, in the course of developing or testing a voting system, facts arise which make the meaning of a particular standard ambiguous or unclear. The EAC may self-initiate such a request when its agents identify a need for interpretation within the program. An interpretation issued by the EAC will serve to clarify what a given standard requires and how to properly evaluate compliance. Ultimately, interpretations do not amend voting system standards, but serve only to clarify existing standards.

9.3. Requirements for Requesting an Interpretation. EAC interpretations are limited in scope. The purpose of the interpretation process is to provide manufacturers, who are in the process of developing a voting system, a means to resolve the meaning of a voting system standard in light of a specific voting system technology without having to present a finished product to EAC for certification. In order to submit a request for interpretation, one must (1) be a proper requester, (2) request interpretation of an applicable voting system standard, (3) present an actual controversy and (4) seek clarification on a matter of unsettled ambiguity.

9.3.1. Proper Requestors. A request for interpretation may only be submitted by a registered manufacturer or agent of the manufacturer acting on its behalf (such as a VSTL). Requests for interpretation will not be accepted from any other party.

9.3.2. Applicable Standard. Requests for interpretation are limited to queries on EAC voting system standards (i.e. VVSG or VSS). Moreover, a manufacturer may only request an interpretation on a version of EAC voting system standards to which the EAC currently offers certification.

9.3.3. Existing Factual Controversy. In order to request an interpretation, a manufacturer must present a question relative to a specific voting system or technology proposed for use in a voting system. Requests for interpretation on hypothetical issues will not be addressed by the EAC. In order to request interpretation, the need for clarification must have arisen from the development or testing of a voting system. A factual controversy exists when an attempt to apply a specific section of the VVSG or VSS to a specific system or piece of technology creates ambiguity.

9.3.4. Unsettled, Ambiguous Matter. Requests for interpretation must involve actual controversies which have not been previously settled. This is a two part requirement:

DRAFT

9.3.4.1. *Actual Ambiguity*. A proper request must contain an actual ambiguity. The interpretation process is not a means to challenge a clear EAC voting system standard. Recommended changes to voting system standards are welcome and may be forwarded to the EAC, but are not part of the Certification Program. An Ambiguity arises when (in applying a voting system standard to a specific technology):

9.3.4.1.1. The language of the standard is unclear on its face;

9.3.4.1.2. One section of the standards seems to contradict another, relevant section;

9.3.4.1.3. The language of the standard, though clear on its face, lacks sufficient detail or breadth to determine its proper application to a particular technology;

9.3.4.1.4. The language of a particular standard, when applied to a specific technology, clearly conflicts with the established purpose or intent of the standard; or

9.3.4.1.5. The language of the standard is clear, but the proper means to assess compliance is unclear.

9.3.4.2. *Not Previously Clarified*. The EAC will not accept a request for interpretation where the issues raised have previously been clarified.

9.4. Procedure for Requesting an Interpretation. Requests for an interpretation shall be made in writing to the Program Director. All requests should be complete and as detailed as possible, as interpretations issued by the EAC are based upon, and limited to, the facts presented. Failure to provide complete information may result in an Interpretation that is off point and ultimately immaterial to the issue at hand. Requests for Interpretation must:

9.4.1. <u>Establish Standing to Make the Request</u>. In order to make a request one must meet the requirements identified in section 9.3, above. Thus the written request must provide sufficient information for the Program Director to conclude that the requestor is (1) a proper requester, (2) requesting interpretation of an applicable voting system standard, (3) presenting an actual factual controversy and (4) seeking clarification on a matter of unsettled ambiguity.

9.4.2. <u>Identify the EAC Voting System Standard to be Clarified</u>. The request must identify the specific standard or standards to which the requestor seeks clarification. The request must state the version of the voting system standards at issue (if applicable) and quote and correctly cite the applicable standards.

9.4.3. <u>State the Facts Giving Rise to the Ambiguity</u>. The request must provide the facts associated with the voting system technology that gave rise to the ambiguity in the

DRAFT

identified standard. The request must be careful to provide all necessary information in a clear and concise fashion. Any interpretation issued by the EAC will be based upon the facts provided.

9.4.4. Identify the Ambiguity. The request must identify the ambiguity it seeks to resolve. The ambiguity shall be identified by stating a concise question. This question:

9.4.4.1. Shall be clearly stated.

9.4.4.2. Shall be related to and reference the voting system standard and voting system technology information provided.

9.4.4.3. *Shall be limited to a single issue*. Each question or issue arising from an ambiguous standard must be stated separately. Compound questions are unacceptable. If multiple issues exist, they should be presented as individual, numbered questions.

9.4.4.4. Shall be stated in a way that can ultimately be answered yes or no.

9.4.5. Provide a Proposed Interpretation. A request for interpretation should propose an answer to the question posed. The answer should interpret the voting system standard in the context of the facts presented. It should also provide the basis and reasoning behind the proposal.

9.5. EAC Action on Request for Interpretation. Upon receipt of a Request for Interpretation the EAC shall:

9.5.1. Review of Request. The Program Director shall review the request to ensure it is complete, clear and meets the requirements of Section 9.3. Upon review the Program Director may:

9.5.1.1. *Request Clarification*. If the Request of Interpretation is incomplete or additional information is otherwise required, the Program Director may send the Manufacturer a request for clarification. This request will identify the additional information required.

9.5.1.2. *Reject the Request for Interpretation*. If the Request for Interpretation does not meet the requirements of Section 9.3 the Program Director may reject it. Such rejection must be provided the Manufacturer in writing and state the basis for the rejection.

9.5.1.3. *Notice Acceptance of the Request*. If the Request of Interpretation is acceptable the Program Director will notify the manufacturer in writing, providing it with an estimated date of completion. Requests for Interpretation may be accepted in whole or in part. A notice of acceptance shall state the issues accepted for interpretation.

DRAFT

9.5.2. Consideration of the Request. Once a Request for Interpretation has been accepted, the matter shall be investigated and researched. Such action may require the EAC to employ technical experts. It may also require the EAC to request additional information from the Manufacturer. The Manufacturer shall respond promptly to such requests.

9.5.3. Interpretation. The Decision Authority shall be responsible for making determinations on requests for interpretation. Once this determination has been made, a written Interpretation shall be sent to the Manufacturer. This written Interpretation shall:

9.5.3.1. State the question or questions investigated;

9.5.3.2. Outline the relevant facts that served as the basis of the Interpretation;

9.5.3.3. Identify the voting system standards interpreted;

9.5.3.4. State the conclusion reached.

9.5.3.5. Inform the Manufacturer of the effect of an interpretation (see Section 9.6, below).

9.6. Effect of Interpretation. Interpretations are fact and case specific. They are not tools of policy, but specific, fact based guidance useful for resolving a particular problem. Ultimately, an interpretation is determinative and conclusive only with regard to the case presented. Nevertheless, interpretations do have some value as precedence. Interpretations published by the EAC shall serve as reliable guidance and authority over identical or similar questions of interpretation. These Interpretations will assist users of EAC voting system standards in understanding and applying its provisions.

9.7. Library of Interpretations. To better serve Manufacturers and those interested in the EAC voting system standards, the Program Director shall select Interpretations for general publication. All proprietary information contained in an Interpretation will be redacted before publication consistent with Chapter 10 of this Manual. The library of published opinions may be found at www.eac.gov.

DRAFT

10.Trade Secret, Confidential Commercial and Personal Information

10.1. Overview. Participants in the Certification Program will be required to provide the EAC a variety of documents, some of these documents may include trade secret, confidential commercial or personal information protected from release by Federal law. This chapter discusses the certification program's standards, processes and requirements that work to identify, document and protect such information from improper release.

10.2. Policy on Trade Secret and Confidential Commercial Information. The Freedom of Information Action (FOIA) and EAC policy promote an open and transparent government process. FOIA generally provides for the release of documents to the public upon request. In most cases, access to government held documents benefit Federal agencies by creating an informed and involved public. However, in some instances the release of information can be harmful to both the individual who submitted it and a Federal agency's ability to perform its mission. Confidential commercial or trade secret information falls into this category. Such information has value in the marketplace. Requiring release of the information would result in competitive harm to its submitter and damage the government's ability to gather such information in the future. Because of this fact, FOIA (5 U.S.C. §522) along with the Trade Secrets Act (18 U.S.C. §1905) protect from public release (1) trade secrets information and (2) privileged or confidential commercial information.

10.3. Trade Secrets. A trade secret is a secret, commercially valuable plan, process, or device that is used for the making or processing of a product and that is the end result of either innovation or substantial effort. It relates to the productive process itself, describing how a product is made. It does not relate to information describing end product capabilities, features, or performance.

10.3.1. For illustrative purposes, examples of trade secrets may include:

10.3.1.1. Plans schematics and other drawings useful in production;

10.3.1.2. Specifications of materials used in production;

10.3.1.3. Voting system source code used to develop or manufacture software where release would reveal actual programming;

10.3.1.4. Technical descriptions of manufacturing processes and other secret information relating directly to the production process.

10.3.2. Examples of documents that are likely not trade secrets include:

10.3.2.1. Information pertaining to a finished products capabilities or features;

10.3.2.2. Information pertaining to a finished products performance.

DRAFT

10.3.2.3. Information regarding product components that would not reveal any commercially valuable information regarding production.

10.4. Privileged or Confidential Commercial Information. Privileged or confidential commercial information is that information submitted by a manufacturer that is *commercial or financial* in nature and *privileged or confidential*.

10.4.1. *Commercial or Financial Information*. The terms "commercial" and "financial" should be given their ordinary meanings. They include records in which a submitting manufacturer has any *commercial interest.*

10.4.2. *Privileged or Confidential*. Commercial or financial information is privileged or confidential if its disclosure would likely cause substantial harm to the competitive position of the submitter. The concept of harm to one's competitive position focuses on harm flowing from a competitor's affirmative use of the proprietary information. It does not include incidental harm associated with upset customers or employees.

10.5. Documents Submitted Voluntarily. Documents submitted voluntarily to a Federal agency are granted a greater degree of protection from public release than those documents submitted involuntarily. Information the EAC requires Manufacturers to submit as a function of the Certification Program are <u>not</u> provided voluntarily. Voluntarily submitted documents are those the manufacturer chooses to submit outside the Certification Program requirements. If a manufacturer wishes to provide such information, it should contact and coordinate with the certification Program Director. If the Program Director determines the information to be voluntary in nature, the manufacturer should label the information appropriately. Such action will prevent the inappropriate or inadvertent release of protected information.

10.6. EAC's Responsibilities. The EAC is ultimately responsible for determining whether or not a document must be released pursuant to Federal law. In doing so, however, the EAC will require information and input from the manufacturers submitting the documents. This is essential for the EAC to identify, track and make determinations on the large volume of documentation it receives. The EAC has the following responsibilities.

10.6.1. Document and information management. The EAC will control the documentation it receives. It will do so in a manner that:

10.6.1.1. Ensures documents are secure and only released to third parties after the appropriate review and determination;

10.6.1.2. Track documents manufactures have previously identified as proprietary and requiring protection under FOIA.

10.6.2. Contact manufacturers upon proposed release of potentially protected documents. In the event a member of the public submits a FOIA request for documents provided by a manufacturer or the EAC otherwise proposes the release of such documents, the EAC will:

DRAFT

10.6.2.1. Review the documents to determine if they are potentially protected from release as trade secrets or confidential commercial information. The documents at issue may have been previously identified as protected by the manufacturer when submitted (see section 10.7.1, below) or identified by the EAC upon review.

10.6.2.2. Grant submitting manufacturer an opportunity to provide input. In the event the information has been identified as potentially protected from release as a trade secret or confidential, commercial information, the EAC will notify the submitter and allow them an opportunity to submit their position on the issue. The submitter shall respond consistent with section 10.7.1, below.

10.6.3. Make a final determination on release. After providing the submitter of the information an opportunity to be heard, the EAC will make a final decision on release. The EAC will inform the submitter of this decision.

10.7. Manufacture's Responsibilities. While the EAC is ultimately responsible for determining if a document, or a portion of it, is protected from release as a trade secret or confidential commercial information, the Manufacturer shall be responsible for identifying documents it believes warrant such protection. This responsibility arises in two situations (1) upon the initial submission of information, and (2) upon notification by the EAC that it is considering the release of potentially protected information.

10.7.1. Initial submission of information. When a manufacturer is submitting documents to the EAC as required by the certification program, it is responsible for identifying any document or portion of a document that it believes is protected from release by law. Examples of submissions required under this program include information submitted during the manufacturer registration process, Technical Data Packages, Test Plans and Test Reports. Manufacturers shall identify protected information by:

10.7.1.1. *Submitting a Notice of Protected Information*. This notice shall identify the document, document page or portion of a page that is believed to be protected from release. This must be done with specificity. For each piece of information identified, state the legal basis for its protected status.

10.7.1.1.1. Cite the applicable law which exempts the information from release.

10.7.1.1.2. Clearly discuss why that legal authority applies and why the document must be protected from release.

10.7.1.1.3. If necessary, provide additional documentation or information. For example, if a document is claimed to contain confidential commercial information, evidence and analysis of the competitive harm that would result upon release would have to be provided.

DRAFT

10.7.1.2. *Label Submissions*. Label all submissions identified in the notice as "Proprietary Commercial Information." Only those submission that are identified as protected should be labeled. Attempts to indiscriminately label all materials as proprietary will render the markings moot.

10.7.2. Notification of potential release. In the event a manufacturer is notified that the EAC is considering the release of information that may be protected, the manufacturer shall:

10.7.2.1. Respond to the notice within 15 days. If additional time is needed, the manufacturer must promptly notify the Program Director. Requests for additional time will be granted only for good cause and must be made before the 15 day deadline. Manufacturers that do not timely respond, will be viewed as not objecting to release.

10.7.2.2. Clearly state in the response:

10.7.2.2.1. That there is no objection to release; OR

10.7.2.2.2. That the manufacturer objects to release. In this case, the response must clearly state which portions of the document are believed to be protected from release. The manufacture shall follow the procedures discussed in section 10.7.1, above.

10.8. Personal Information. Certain personal information is protected from release under FOIA and the Privacy Act (5 U.S.C. §552a). This information includes private information about a person which if released would cause the individual embarrassment or constitute and unwarranted invasion of personal privacy. Generally, the EAC will not require the submission of private information about individuals. The incidental submission of such information should be avoided. If a manufacturer believes it is required to submit such information, it should contact the Program Director. If the information will be submitted, it must be properly identified. Examples of such information include:

10.8.1. Social Security Numbers;

10.8.2. Bank account numbers;

10.8.3. Home addresses and

10.8.4. Home phone numbers.

DRAFT

Appendix A

Manufacturers' Registration Form

Available in electronic format at www.eac.gov

DRAFT

DRAFT

Appendix B

Voting System Certification Application Form

Available in electronic format at www.eac.gov

Appendix C

Discussion of Practices: Delivery and Validation of Trusted Voting System Software

DRAFT

Delivery and Validation of Trusted Voting System Software

Overview

This document discusses the design of a proposed system for delivery and validation of trusted voting system software and the rational for this system. The purpose of the system is to provide a high level of confidence that software used in elections is a faithful and unmodified copy of the certified version. This foundation of trust is built upon two pillars. The first pillar is that the certification process is effective and will prevent deficient or malicious software from being approved. The second pillar, and the subject of this document, is that the software that was certified is what is being used in elections and can be verified as that.

We begin with a discussion of how software is built and delivered. Next the security risks of the system are discussed and the security principles used to protect the system are set forth. The main part of the document then discusses how those security principles are or could be implemented to protect the delivery of voting system software. In some cases the features described future possibilities. In other cases features are already in use in some states, but not in others.

Building and Delivering Software

Computers only understand numbers. In fact they only understand 1’s and 0’s. This is called binary coding. Back in ancient computing times, (the 1950’s and 1960’s), some people actually wrote computer programs as long strings of numbers. The computer’s central processing unit (CPU) that understood certain numbers were instructions for different actions like add, subtract, read memory or write to the disk. It also understood that some of the numbers were its data. For example the number that meant read memory would be followed by a number that wasn’t another instruction but pointed to the location in the memory to be read.

People soon grew tired of writing computer programs as long lists of numbers and so computer languages were developed. These computer languages were meant to allow people to write programs in something that looked more like speech. So now programmers would write lists of commands like “read”, “print” or “if..else..”

However, the computers still only understood numbers so a special program was developed that translated the programming instructions to the numbers the computer would understand. This program is usually called a compiler and the process of converting the programming instructions into the numbers a computer can read is called a compilation or a build. The result of a build is called executable code, because it is in a form the computer can execute.

Today computer programmers use very sophisticated computer languages to write programs. Some of these languages even start to look like human language, if you are a computer geek. These programs are called source code because they are the input or source for the next steps in

DRAFT

the process. When they are ready they use a compiler to build their program into executable code and run it on a computer. So the steps in the process are:

1. Write a source code program in computer language.
2. Build the source code into executable code.
3. Take the executable code to a computer.
4. Load the executable onto the computer and run it.

This is all pretty simple. Now let's see what could go wrong.

Securing the System

Once the system for producing, delivering and installing executable code is understood the system must be examined to identify any security vulnerabilities. The first step in a security analysis is to develop a threat model. What are we worried about? What threat do we need to protect the system against?

We could hypothesize a conspiracy involving two or more people. However, large conspiracies are almost impossible to keep secret. Even two people, if they work for different organizations, are hard to co-opt successfully. Once you start assuming that a conspiracy is possible then the situation starts becoming increasingly complex and there is more debate over how likely that is to happen. Debating the possibility of conspiracy scenarios is not within the scope of this document. Everyone seems to agree that the system should be protected in a way that one rogue employee could not do anything bad without being detected.

Once we have agreed on the threats then we can talk about how to protect the system from those threats. Developing a complete security system is a very complex and involved task. This document only focuses on some of the issues that are important for protecting the production, delivery and installation of executable code in a voting system.

The Threat Model

So what are we worried about? There are many, many possible answers to that question. This document deals with preventing a single threat of a rogue actor in the system. Let's assume we may get a rogue person who wants to manipulate the voting system. An insider probably has the most potential for doing damage, so let's assume this person is an employee of an organization that is involved with the voting system. The person may work for a local elections office, an equipment manufacturer, a test house or any other organization that deals with voting equipment.

What could one rogue employee do and how would we protect the system against them?

Security Principles

DRAFT

The system should be designed with multiple protections. This is called a defense in depth. Some of these protections will try and prevent a malicious person from doing what they want to do. Other features will try and detect if somehow they were able to do it anyway. Still other features will document what happened and provide evidence in an investigation if there is ever suspicion that something bad happened.

Multiple Independent Knowledgeable Witnesses

One principle the system should follow is that nothing is done without multiple, independent and knowledgeable witnesses. At least two witnesses should be present at every step in the process. Witnesses should be independent of each other, meaning they work for different organizations and don't have any connection other than coming together to to complete a task related to the voting system. Both of our witnesses should be sufficiently knowledgeable about the task so that they can be expected to spot an action that might potentially compromise the system.
The first principle then is that every action in the process must be witnesses by two or more people, from different organizations who understand what is being done.

Documented Chain of Custody

A voting system should have a documented chain of custody. Officials should be able to track the software on a voting system back to the source code that was delivered to the national lab for certification. We want to be able to prove that the executable code used in an election is exactly the same as that certified at the national and state level.

Protection, Detection and Recording Mechanisms

A voting system should also have multiple levels of protection. It isn't unusual for our homes to have locks on the door, a light on the porch, a dog and, for some, a shotgun under the bed. That is one form of defense in depth. A thief might easily get by any one of those things but together they make it reasonably hard and potentially unpleasant for a thief to successfully break in. Similarly the voting system should also have multiple levels of protection. Some features will prevent something bad from happening. Other features will serve to detect if somehow the system is compromised. If the protections work, the detection features should never be needed. However, we live in an imperfect world so we need to provide for both prevention and detection. Even more, we want good records so that if there is ever a reason to investigate we can prove or disprove that the system worked. If these records show that despite all of the protections, someone corrupted the system, then the courts can decide the appropriate action. The system should be able to give the courts the evidence to determine what has happened.

Security System Design

A certification system with three major elements flows from our security discussion. These elements are:

- Build source code into executable code

DRAFT

- Delivery unmodified version of the executable code to state and local authorities
- Verify that the code in use is unmodified from the certified code

To accomplish our security objectives the following principles are applied to each step of the process:

- Multiple independent knowledgeable witnesses
- Documented chain of custody
- Protection, detection and recording mechanisms

The application of these security principles to the different stages of the delivery process gives us the system design that will be discussed in the remainder of this document.

Source Code Review

The first step in the process is an independent review of the source code. This is a requirement for national certification and also for some State certifications. This is one example of using multiple independent witnesses in which the manufacturer's programmer writes the programs for the voting system and then the national test lab review those programs, line-by-line, to make sure they do what they are supposed to do and only what they are supposed to do.

After the source code is built into executable code, there is testing of the software as it is used in a voting system. The source code review, together with the operational testing, provides multiple checks that the software operates correctly and doesn't have hidden code in it.

Building Software

Once the source code has been reviewed by the national laboratory it must be compiled to build the executable code that will actually run on the voting system. A software build is a complex process and a lot goes on under the control of the computer during the process. When this process is completed, we need to be very confident that the source code reviewed is exactly what is in the executable code that is produced and that there hasn't been anything else added. This is easier said that done, but let's take a look at some options.

Witness Build

The national certification system, under NASED and the ITA's, required a witness build. The manufacturer delivered source code to the ITA. The source code was reviewed. Then the manufacturer with a witness from the ITA performed the build. The executable code created was then loaded onto the machines and the rest of the testing on the voting system was performed. This system was a great improvement over what had existed before, which was no national certification system. Prior to the NASED national certification system every state conducted its own system review with very uneven levels of scrutiny.

DRAFT

There are notable weaknesses in the witness build process. First, the manufacturer's employee provided the build environment, without any kind of qualification. A computer loaded with a build environment is a very complex environment with numerous files and programs. It is quite conceivable that someone could hide some additional software module and instructions to insert that software into the executable code. The ITA's witness and even the manufacturer's employee who performs the build might perform the build in good conscience, unaware that more was happening than they were aware of.

A second major weakness is that the records of the build process were inadequate to recreate it. If at a later time there was a need to investigate an allegation the records of the witness build process have been insufficient to recreate the original build environment or validate that the build environment is unchanged from that which was originally used.

A third weakness is that the witness build, while valuable, was not constructed with a view to its being an important part of a verifiable chain of custody from the national certification process to the software used in an election.

Trusted Build

The concept of a trusted build may be considered a generational revision of the original witness build. The trusted build is constructed with the intent that it serve as an important component of a verifiable chain of custody. The role of the test authority witness is revised to make them the primary operator of the build process. Records and file signatures are significantly enhanced to allow recreation of the build environment and verification that the original build environment has been reproduced without modification. Significant added supervision is given to the creation of the build environment itself to assure that the environment itself is free of unknown elements.

The trusted build, depicted in Figure 1, begins with delivery of the source code from the manufacturer. The source code is reviewed for compliance with the EAC's applicable voting systems standards. File signatures of the source code modules are produced and recorded.

The build environment is then constructed. The disk that will hold the environment is completely erased using special software that assures complete and total cleaning of the disk, including the root sectors. It is preferred that the build environment be created by test authority personnel using commercial software purchased by them from the open market. Once the build environment is created its file signature is recorded so that if there is ever a need to recreated it the fidelity of the recreation may be verified.

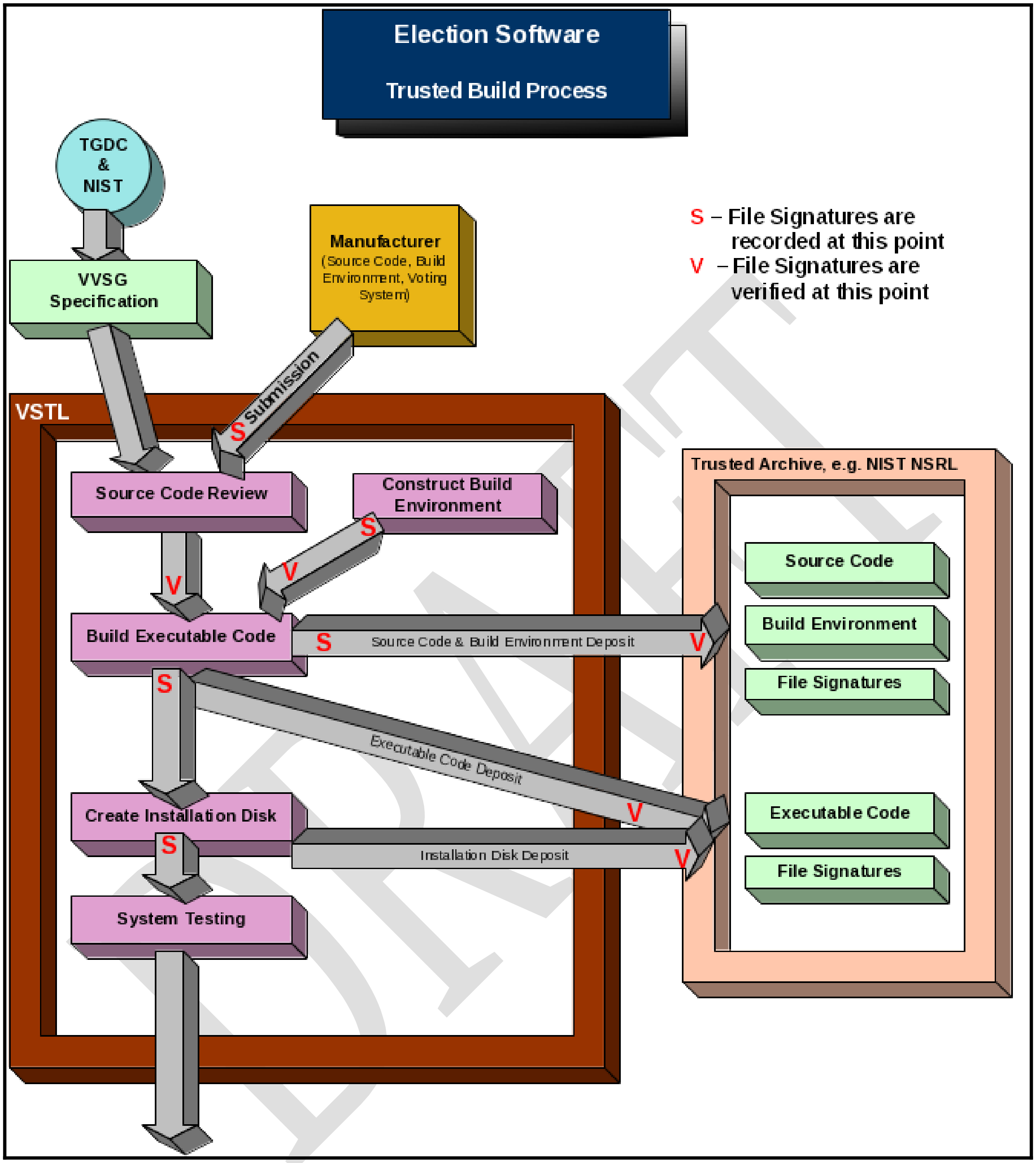
After the source code has successfully passed the source code review it is time to perform the build. First the file signatures of the source code modules and the build environment are checked to assure that they are unchanged from their original form. Then the source code is loaded onto the build environment and file signatures are taken of the resulting combination. A disk image is also taken of the combination just before the build is performed. The disk image is archived in a trusted archive to assure that the build can be reproduced should there ever be a need to do so. Having this disk image available is a great help in incorporating modifications to software. For modifications, having the original build environment allows focus on only the modified software

DRAFT

modules. The rest of the modules can be verified as unchanged and therefore can be trusted based on the original certification.

The executable code is then produced. File signatures of the executable code are taken and recorded. The executable code is then archived and also used to create installation disks. File signatures are also taken of the installation disks so that they may be validated by those who will later install the software into voting systems.

DRAFT


Election Software
Trusted Build Process
TGDC & NIST
VVSG Specification
Manufacturer (Source Code, Build Environment, Voting System)
S – File Signatures are recorded at this point
V – File Signatures are verified at this point
VSTL
Submission
S
Source Code Review
Construct Build Environment
S
V
V
Build Executable Code
S
Source Code & Build Environment Deposit
V
S
Executable Code Deposit
V
Create Installation Disk
S
Installation Disk Deposit
V
System Testing
Trusted Archive, e.g. NIST NSRL
Source Code
Build Environment
File Signatures
Executable Code
File Signatures

DRAFT

Figure 1 – The Trusted Build Process

The executable code is then installed on the system submitted for certification and the rest of the certification testing is performed.

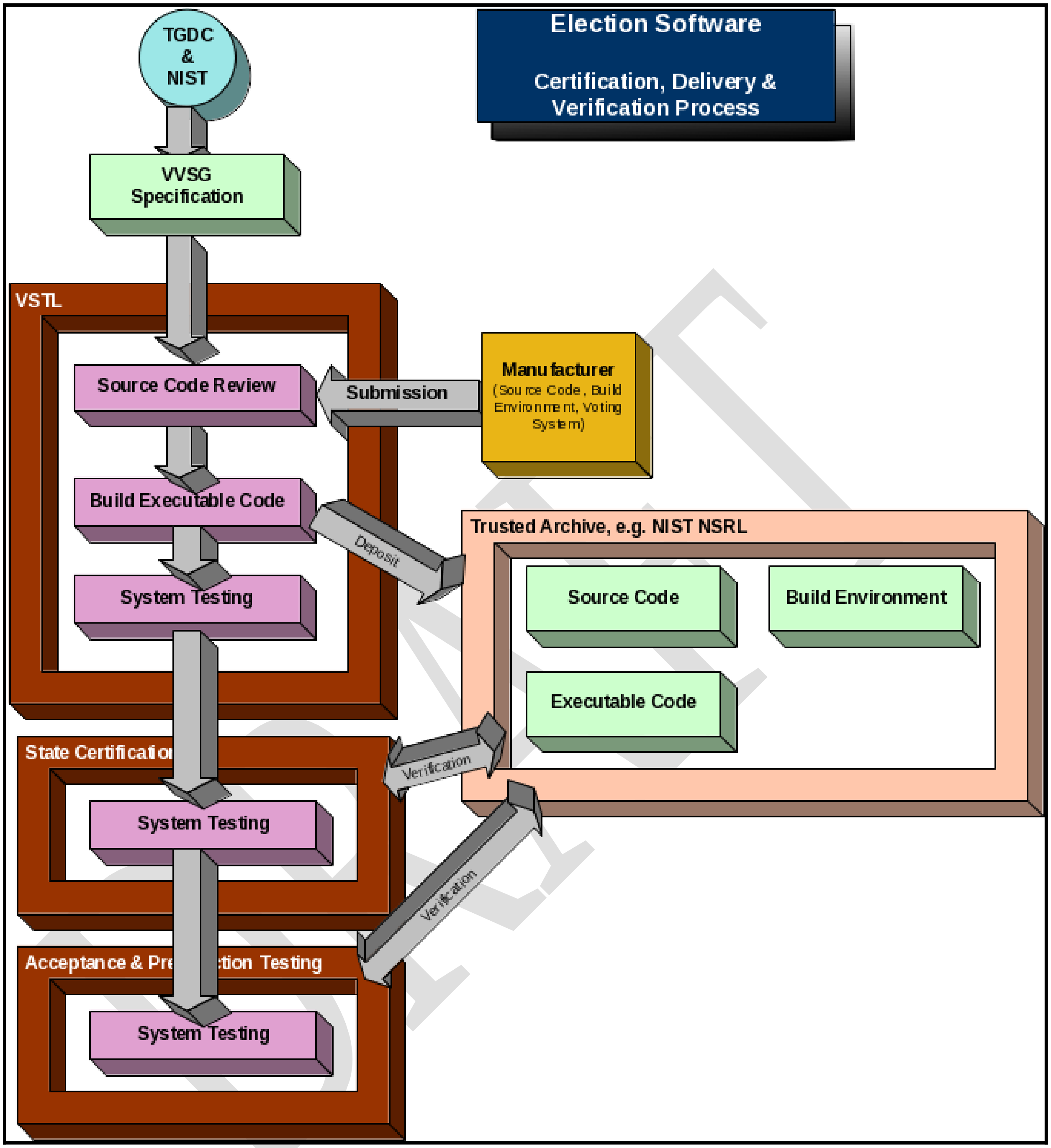
The combination of recording file signatures and using trusted archives allows a well documented chain of custody to the end user of the software and a mechanism for the end user to independently verify that the software loaded onto their voting systems is unmodified from the certified version.

Protecting Delivery

Delivery of voting system software is challenging because of the wide geographical distribution of users and the many different scenarios under which new software is required. In some cases large purchases are made of new voting systems. Typically the purchasing authority wants complete delivery of system as ready to use as possible. In these circumstances the purchaser would prefer that the software be installed before delivering the systems. Independent verification that the installed software is unmodified from the certified version is particularly important in this case. In other situations new software version must be delivered and installed on equipment already deployed for use.

Regardless of the scenario there should be carefully constructed and documented delivery of the software from the source through installation on the equipment. Once the software is installed the voting systems should be locked with tamper-proof seals and maintained under careful physical security. These requirements are part of good election administration, and are mentioned simply to highlight the role election administration plays in conjunction with the certification process to safeguard the election system.

DRAFT



DRAFT

Figure 2 – Process Model for the Certification, Delivery and Verification of Voting System Software

Verifying Delivery

Value of File Signatures

File signatures, commonly called HASH codes, are a valuable tool for verifying that the chain of custody has not been violated. File signatures give a high confidence that the software being used has not been modified from the version that was certified. They can be used by local election administrators to assure that the software to be used in an election is identical to what was certified and that no modifications have been made.

It is recommended that the file signatures be check and confirmed a critical junctures in the process. State officials should check file signatures as part of conducting a state examination. When this is done it creates an independent verification that the chain of custody performed properly.

Trusted Archive

Archiving of information is an important function. It creates a trusted source to hold certified software. When the file signatures are made available independent verification of software is possible. Further archiving provides a secure record providing detailed evidence should serious allegations need to be investigated.

On-Site Signature Verification

It is recommended that when practical the file signatures of the software used in elections be confirmed before every election. This simple mechanism serves to document that software is unmodified. If the signatures do not conform then an investigation will be required and further actions necessary to assure that only certified software is used in an election.

3rd Party Signature Verification

An additional feature could be the use of 3rd party verification of file signatures. Checks of software file signatures sometimes requires special equipment and expertise. For example once firmware has been loaded onto chips on a printed circuit board it may require special equipment to verify that the loaded software is a correct copy of the certified version.

A 3rd party verification also provides another independent witness along with other security features. If in addition to on-site signature verification an appropriately delegated official randomly selects and sends copies of software to a trusted and independent 3rd party then an additional level of verification can be created.

Private/Public Key Encryption

The use of Private/Pubic Key encryption may offer some real benefits in assuring that only trusted software is loaded onto a voting system. If the system itself or election officials require that only software that can be authenticated through a public encryption key be installed then

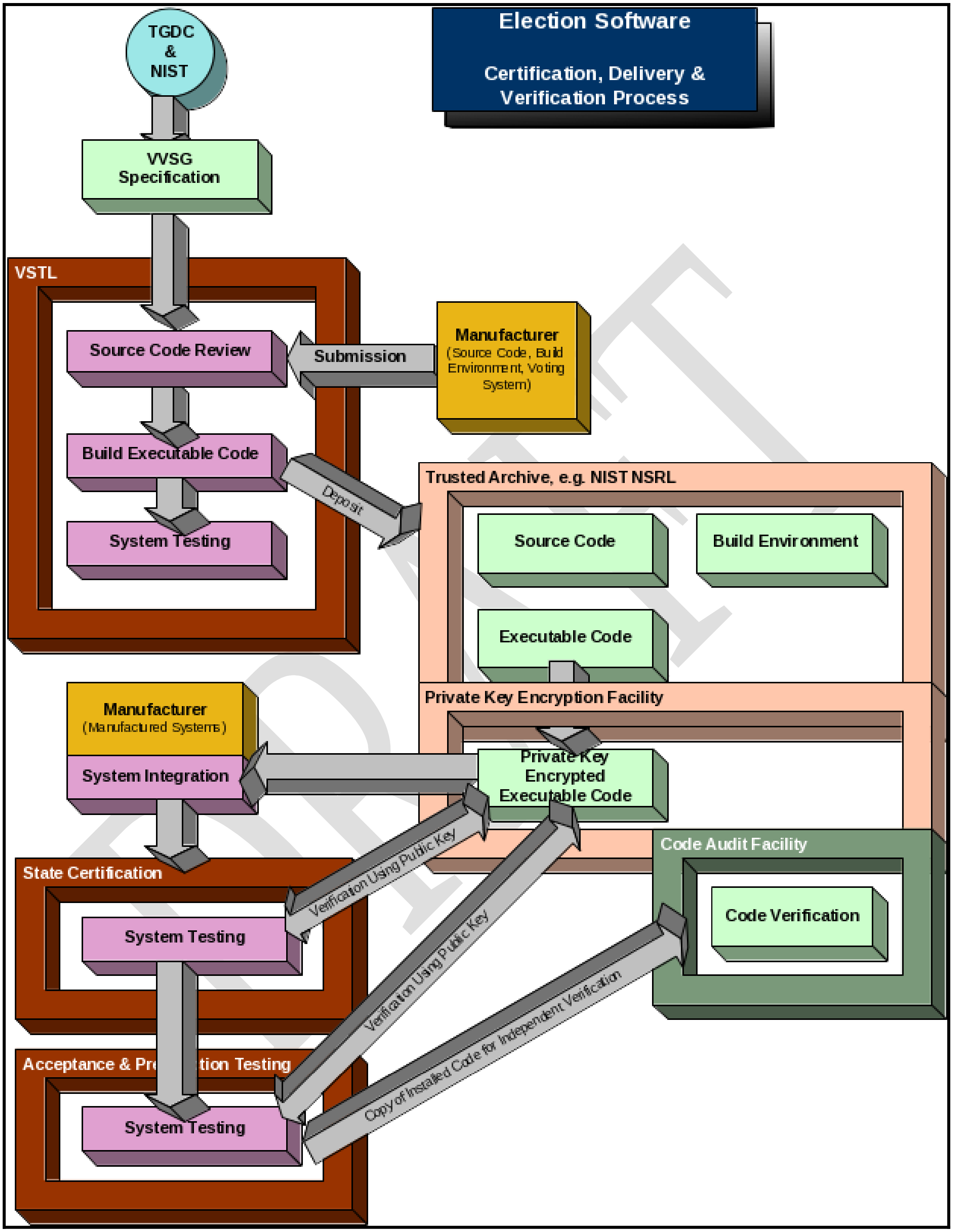
DRAFT

confidence is gained that the software has been encrypted by the corresponding private key. The private key would be carefully guarded by the EAC or state officials. This could be a simple mechanism to protect voting system software during transport from being modified.

Vulnerabilities in this mechanism are that the private key might be switched with another that would allow modified software to be loaded. Further the key validation software might be compromised to allow software encrypted by either of two keys to be loaded.

The protections against these vulnerabilities are the other security features of the system, e.g. the validation of file signatures after the software is loaded and the physical security used throughout the process. An alternative could be to return the software after it is loaded to the source or another trusted party to have an audit check of the software that was loaded. As long as the process and people involved in receiving the software were different from those sending back the software to be audited there is additional confidence that the software loaded was a faithful copy of the certified software.

DRAFT


Election Software
Certification, Delivery & Verification Process
TGDC & NIST
VVSG Specification
VSTL
Source Code Review
Build Executable Code
System Testing
Submission
Manufacturer (Source Code, Build Environment, Voting System)
Deposit
Trusted Archive, e.g. NIST NSRL
Source Code
Build Environment
Executable Code
Private Key Encryption Facility
Private Key Encrypted Executable Code
Manufacturer (Manufactured Systems)
System Integration
State Certification
System Testing
Verification Using Public Key
Verification Using Public Key
Code Audit Facility
Code Verification
Acceptance & Pre[illegible]tion Testing
System Testing
Copy of Installed Code for Independent Verification

DRAFT

Figure 3 – Integration of PKI to delivery and verification process

Preserving Evidence

DRAFT

The system described in this document makes extensive use of trusted archives and retains more material than is the practice currently. Specifically the following items are archived:

- The source code
- The build environment (pre and post build)
- The executable code
- The installation disks

Archiving these items provides evidence for any future investigations. Further these archives support other features of the system such as having 3rd party delivery of software after it is certified.

Compounding Confidence

The certification process for voting equipment in the United States is a diverse system with federal, state and local participation. The design of the total system is that confidence is build as different participants perform their function and build increasing confidence. On the national level the EAC certification program assures that systems meet the technical standards established by the EAC. State certification efforts take an independent look at the same system and assure that the system meets the specific requirements of individual states. Local evaluation testing focuses on selecting the best system for a particular jurisdiction. Finally acceptance testing is intended to assure that the equipment received is in good operating condition and is identical to that certified on the national and state level.

Conclusion

The voting system software deliver and validation system provides a safe and effective system, to assure that the software used in elections can be trusted. The system provides multiple security features, creating a defense in depth of the system. Some features are intended to assure that only certified software is delivered for use in voting systems. Other features are intended to detect if the system ever fails in any way to use certified software. Careful records and archiving provide trusted 3rd party sources for software and preserve evidence should investigations become necessary.

To achieve these ends the system for delivering and verifying voting system software has been analyzed as having three major components:

- Build source code into executable code
- Delivery unmodified version of the executable code to state and local authorities
- Verify that the code in use is unmodified from the certified code

The security objectives have been implemented by following the principles of:

- Multiple independent knowledgeable witnesses
- Documented chain of custody

- Protection, detection and recording mechanisms

The features suggested intend to first create a high confidence that the build process faithfully transforms the source code into executable code without any additional code or modifications being introduced. From the trusted build we then turn our attention to the delivery process. File signatures are recorded at the end of the build process. These allow verification of the code as it is delivered for use. Trusted archiving is used to give confidence that faithful copies of the source and executable code are available. Archiving further creates evidence that can later be used in investigations. Taken together these features create a robust system to assure that the software used in elections can be trusted.

DRAFT

Appendix D

Field Anomaly Reporting Form

Available in electronic format at www.eac.gov

DRAFT